Document Number 102-94-007U

4

Technical Report

Analysis of End-to-End Encryption and Traffic Flow Confidentiality Options

Task 3
Contract No. N00039-93-C-0099
CDRL No. A003

April 20, 1994

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 51)
Arlington, VA 22245-5200

Prepared by:

Secure Solutions, Inc.
9404 Genesee Avenue, Suite 237
La Jolla, CA 92037
(619) 546-8616

Document Number 102-94-007U

Technical Report

Analysis of End-to-End Encryption and Traffic Flow Confidentiality Options

Task 3
Contract No. N00039-93-C-0099
CDRL No. A003

April 20, 1994

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 51)
Arlington, VA 22245-5200

Prepared by:

Secure Solutions, Inc.
9404 Genesee Avenue, Suite 237
La Jolla, CA 92037
(619) 546-8616

This Page Intentionally Left Blank

Table of Contents

Appendices

Index of Figures

Index of Tables

This Page Intentionally Left Blank

Executive Summary

Secure Solutions, Inc. was tasked by the Space and Naval Warfare Systems Command (SPAWAR) to perform a Small Business Innovation Research (SBIR) Phase II network security research effort.

The use of end-to-end encryption (E^3) services in internetworks where the trustworthiness of intermediate subnetworks is not provided is a critical capability for the Navy. The data to be transferred from the source host to the destination host can be encrypted at the source and not be decrypted until it reaches the destination. Advantages of using end-to-end encryption in internetworks could include the flexibility to connect classified hosts to commercial networks. Even if the data traverses subnetworks or components that are not trustworthy, the data still retains its assurance of confidentiality so long as the encryption keys are not compromised and the encryption algorithm is sufficient to preclude a cryptanalytic attack.

Although end-to-end encryption protects the user data from observation, it does not safeguard against traffic flow leakage from protocol headers that are applied after the end-to-end encryption is performed. Security-relevant information that may be available in the headers or derived from the headers includes source and destination addresses, priorities, security labels, message lengths, transmission frequencies, sequence numbers, flow control information, message routing lists, lifetime of the *protocol data unit* (PDUs), and checksums. It is necessary to determine the extent of the vulnerabilities associated with sending headers in the clear in order to eliminate or reduce the traffic flow confidentiality problem. The nature of this information provides a basis for determining the advantages and disadvantages of providing traffic flow confidentiality services at the lower layers after the headers have been applied.

Task 3, as documented in this report, analyzes protocol control information associated with local area network (LAN) and wide area network (WAN) communication protocols and assesses what information can be derived from the protocol headers through traffic analysis, which is the inference of information from observation of traffic flows (e.g., their presence, absence, amount, direction, route, frequency, time of transfer, length, and other security-relevant information).

The report describes the utility of traffic flow confidentiality options that may be employed to reduce the risk of exposure to traffic analysis. The primary measure to implement traffic flow confidentiality is the prevention of direct observation of information. This is accomplished with a confidentiality service, i.e., through the use of encryption for most networks or a protected distribution system for some links of a network. In addition, the ability for an adversarial traffic analyst to derive information must be prevented. This is accomplished through the insertion of dummy traffic, data padding, route control, data unit segmentation, address hiding, and timing techniques. The padding mechanisms must be implemented before the confidentiality mechanisms in order to be effective.

The major conclusions of this task 3 study are:

- In most environments, the implementation of traffic flow confidentiality is unwarranted due to the processing overhead that is associated with it.
- In those cases where traffic flow confidentiality is warranted, it may be advisable to implement a combination of mechanisms at different layers. The OSI Security Architecture, ISO 7498-2, identifies the layers at which traffic flow confidentiality can be provided: the Application Layer, Network Layer, and Physical Layer.
- Implementation of traffic flow confidentiality at the Application Layer will allow the user to be selective. In addition, it provides end-to-end (user-to-user) service. By implementing traffic flow confidentiality at a lower layer, traffic flows for the End System as a whole can be masked. In most cases, implementation of one or the other is sufficient, depending on whether traffic flow confidentiality is desired for the entire host or for selective applications on the host, or even selective traffic processed by the application.
- Data padding performed at the Application Layer is the first step in effectively concealing message sizes and types. Data padding can also be accomplished at the Transport, Network, and Data Link Layers, perhaps with less impact because it would not be applied to individual applications. However, the Network Layer Security Protocol is the only security protocol that is specifically designed to perform data padding for traffic flow confidentiality.
- When padding is accomplished at the Application Layer, encipherment will be accomplished at the Presentation Layer after context translation. When padding is accomplished at the Network Layer, encipherment can be accomplished immediately after by the same protocol entity.
- SDE can be used at the Data Link Layer to encapsulate CLNP and LLC headers on LANs. Although the OSI Security Architecture does not call for traffic flow confidentiality services at the Data Link Layer, SDE can provide limited traffic flow confidentiality within a LAN, or across multiple LANs connected by remote bridges. What remains exposed to observation by other nodes on the LAN are the MAC addresses, and time and frequency of transmission. Since SDE cannot be implemented with WAN protocols, X.25 and LAPB headers expose some information that can only be protected at the Physical Layer.
- Traffic padding can generate dummy traffic between two End Systems or any segment of a network to help camouflage heavy traffic loads. While traffic padding is an important traffic flow confidentiality mechanism, it incurs much overhead because connections must be padded to near capacity in order to conceal when peak traffic actually exists.
- Timing techniques to delay low priority messages can be employed when there is heavy traffic so the load appears to stay at an even level.

- Segmentation with encryption conceals the original size of data units formed by application processes. Segmentation is performed by some Application Layer protocols, TP4, TP1, NLSP, CLNP, X.25, and SDE.
- Route control, provided by CLNP, is an effective support mechanism to help ensure that traffic is not routed over insecure subnetworks or components. It can also be used to disperse PDUs and PDU segments over diverse paths. However, traffic analysts may still be able to recognize when traffic between two particular hosts is high if addresses or PDU types can be identified, even though they cannot observe the full load. Route control requires the use of additional fields in the PDU to explicitly identify the path to be traversed. If a security protocol is used to encapsulate the CLNP header, an additional CLNP protocol header may be needed below the security protocol to implement route control over the untrusted portion of the internetwork. For these reasons, there is significant overhead associated with route control.
- CLNP headers contain information that a traffic analysts can use to recognize when particular activities are underway at the source and destination organizations. Therefore, it is preferable to implement NLSP or SP3 below CLNP in environments where the security protocol peer entities are End Systems so the actual addressee can be hidden.
- Another reason for implementing NLSP or SP3 below CLNP is that CLNP has a lifetime field (i.e., expiration counter) in the header that is decremented by each Intermediate System and used to eliminate expired PDUs from the network. An adversary could modify the lifetime field in order to flood a network or to cause messages to expire before they arrive at their destination and still maintain the normal traffic flow out of the adversarial station.
- FDDI can be protected by physical means or through full period encryption on each point-to-point link.
- CSMA/CD can be partially protected with full period encryption, but the preamble and starting delimiter must be sent in the clear to achieve bit and frame synchronization.
- Full traffic flow confidentiality can only be provided at the Physical Layer in certain circumstances: two-way simultaneous (full-duplex), synchronous, point-to-point transmission. Full traffic flow confidentiality is not effective against active threats unless integrity mechanisms are also utilized in a cooperative manner.
- A mechanism that offers a high degree of protection from wiretapping of the link between two remote bridges which are in close proximity is a Protected Distribution System. However, a PDS would not protect traffic from observation by other stations on a LAN. Full period encryption provides a similar service when the remote bridges are geographically remote.

The recommendations of this task 3 study are:

- Implement traffic flow confidentiality mechanisms only when absolutely necessary because they require significant overhead and may cause network congestion.
- Consider implementation of a combination of mechanisms at different layers.
- Avoid the use of route control for traffic flow confidentiality due to excessive overhead associated with its use and the need for two CLNP headers when a security protocol is applied below the upper CLNP header.
- Application Layer traffic padding mechanisms should be reserved for those sites or applications that are determined to have traffic profiles which can be used to infer classified missions or information.
- When traffic flow confidentiality is deemed necessary, the protocol stack should primarily include traffic flow confidentiality at the Network Layer for internetwork traffic, and at the Data Link Layer, when possible, for traffic contained within the LAN.
- Traffic flow confidentiality on a link basis should be more widely implemented for the links that connect End Systems to an internetwork. This can be implemented most robustly using full period encryption. An alternative that is feasible for some sites is to use physical security measures such as a PDS.
- The link between LANs that are connected by remote bridges should be protected by full period encryption or a PDS.

Section 1

Introduction

This Page Intentionally Left Blank

1.0 Introduction

This task 3 report documents the results of an analysis performed by Secure Solutions under the Small Business Innovation Research (SBIR) Program for the Department of the Navy's Space and Naval Warfare Systems Command (SPAWAR) under Contract Number N00039-93-C-0099. The report describes the utility of traffic flow confidentiality options that may be employed to reduce the risk of exposure to traffic analysis.

This introduction to the report provides background information on why this research effort was initiated, the scope and objectives of the study, the approach used, and the organization of the report.

1.1 Background

Naval command and control systems are hosted on ship, submarine, shore, airborne, and space platforms that operate in a variety of environments. Diverse communication networks are used to support these command and control systems. These networks operate from the Extremely Low Frequency (ELF) to Extremely High Frequency (EHF) bands and employ both point-to-point and broadcast transmission techniques. A major thrust in Naval command and control is to interconnect these networks for the purpose of sharing information and improving the survivability of the overall network.

To support application-level interoperability among command and control systems which use these networks, the use of a layered architecture is imperative. [Copernicus 91] The most well-known framework for a layered architecture is the International Standards Organization (ISO) seven layer Open Systems Interconnection (OSI) Reference Model (RM), as described in ISO 7498. [ISO 84] It is critical for the Navy that placement of security services be done in a manner that conserves bandwidth, supports real-time transmission requirements, promotes survivability and availability, and supports the security services.

The use of end-to-end encryption (E^3) services in internetworks where the trustworthiness of intermediate subnetworks is not provided is a critical capability for the Navy. Advantages of using end-to-end encryption in internetworks could include the flexibility to connect classified hosts to commercial networks. If the encryption mechanism is implemented at one of the higher layers of the OSI RM, the data to be transferred from the source host to the destination host can be encrypted at the source and not be decrypted until it reaches the destination. If the source and destination hosts are the only entities in the network that hold common keys for a symmetric cipher system, or if the destination host is the only entity in the network that holds the secret key that corresponds to the public key that was used by the source to encrypt the data for an asymmetric cipher system, then no other entity within or external to the network can decrypt the data at any intermediate point. This means that even if the data traverses subnetworks or components that are not trustworthy, the data still retains its

assurance of confidentiality so long as the key is not compromised and the encryption algorithm is sufficient to preclude a cryptanalytic attack.

The implementation of end-to-end encryption as a trusted operating system service could be accomplished more efficiently than some approaches currently being used, such as inserting an encryption device between hosts and the network. However, the use of end-to-end encryption does not safeguard against traffic flow leakage from protocol headers that are applied below the point where end-to-end encryption was performed, since they are not encrypted and may contain or allow one to infer security-relevant information.

The nature of the protocol control information available at lower layers provides a basis for determining the advantages and disadvantages of providing link encryption at the different lower layers. It is necessary to determine the extent of the vulnerabilities associated with sending lower layer OSI headers in the clear in order to eliminate or reduce the traffic flow confidentiality problem.

This task, Task 3 of the SBIR Phase II effort, analyzes protocol control information associated with local area network (LAN) and wide area network (WAN) communication protocols and assesses what information can be derived from the protocol headers through traffic analysis. Traffic flow confidentiality options that can be implemented to reduce the risk are then discussed and analyzed.

Figure 1.1-1 illustrates the layers of the OSI RM and how data is processed at each layer while being transferred between sending and receiving application processes on Hosts A and B through a single relay. In practice, there may be many relays between the source and destination hosts, and they could be for other layers than just the Network Layer, as shown in the illustrative example. The transfer begins when an application process on Host A passes data to the Application Layer for the application process on Host B. The application protocol entity within the Application Layer prepends an application header to the data and then passes the combination of the application header and application data down to the Presentation Layer. The presentation protocol entity within the Presentation Layer then prepends a presentation header to this data and passes the result down to the Session Layer. This process continues at Host A until the data reaches the Physical Layer and is then transmitted over the physical link to the relay.

At the relay, protocol headers are processed and removed as the received data moves up the protocol stack from the Physical Layer to the Network Layer. At the Network Layer, a routing decision is made and new headers are prepended as the data flows down the protocol stack and over another physical link to Host B.

At Host B, all protocol headers are processed and removed as the data flows up the protocol stack from the Physical Layer to the Application Layer and ultimately on to the application process. As illustrated in the figure, correspondent protocol entities in Layers 4 through 7 are located at the source and destination hosts, and not in the relay.

Correspondent protocol entities at Layers 1 through 3, on the other hand, lie at either end of each physical link (e.g., from host-to-relay and relay-to-host).

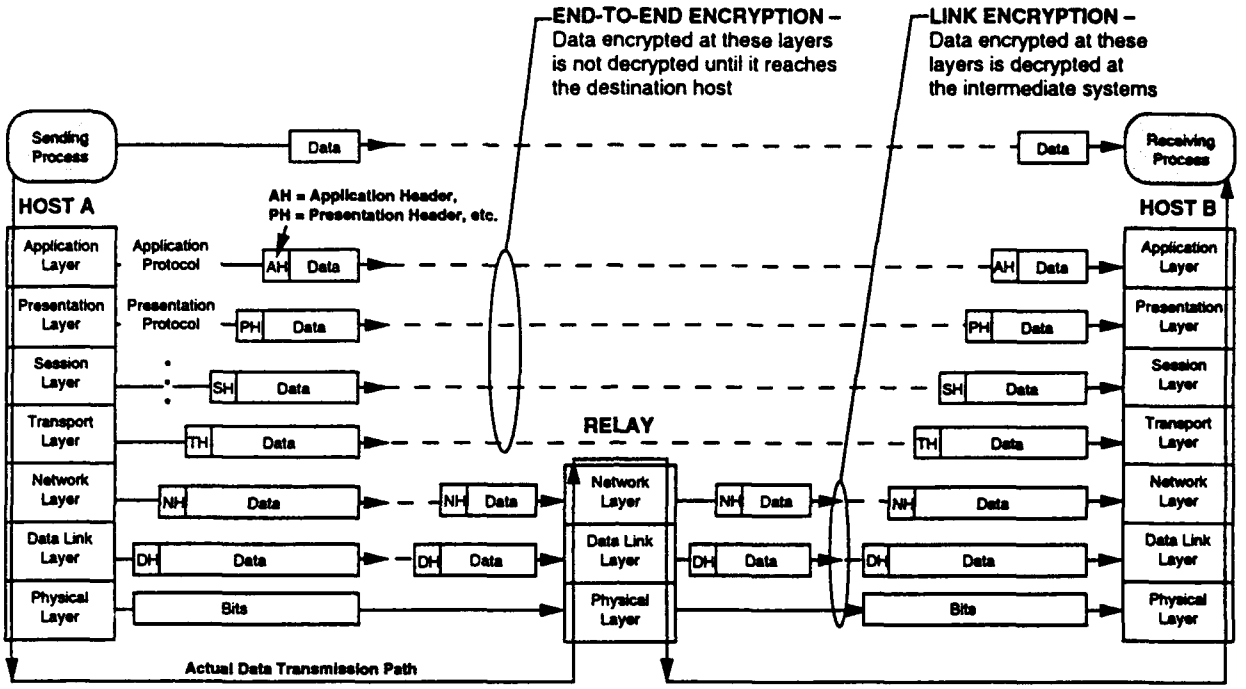


Figure 1.1-1. Headers Processed

Therefore, to provide end-to-end encryption services, the encryption mechanism should either be implemented within the application process itself or in protocol entities that lie within Layers 4 through 7. While these observations are accurate with regard to the definitions of OSI RM connectivity, it is also noted that the Network Layer Security Protocol (NLSP) and the Secure Data Network System (SDNS) Security Protocol 3 (SP3) do optionally provide end-to-end encryption services at the top of Layer 3.

1.2 Scope

This task 3 study analyzes the traffic flow confidentiality features of the following security protocols:

- Transport Layer Security Protocol (TLSP)
- SDNS Security Protocol 4 (SP4)
- Network Layer Security Protocol (NLSP)

- SDNS Security Protocol 3 (SP3)
- Interoperable LAN / MAN Secure Data Exchange (SDE).

The Key Management Protocol and Message Security Protocol (MSP) were not analyzed since they are not general-purpose security protocols.

The security protocols augment other communications protocols. While this study is focused on the security protocols, some standard communications protocols must be included in the protocol stacks in order to effect transmission and receipt of message traffic. It is necessary to analyze the information available in the headers of these protocols in order to determine what security-relevant inform may be available for interception if security is applied only by the application pro or at the Application Layer, and to compare that with what security-relevant informa on may be available for interception if security is applied at other layers.

To limit the scope of this effort, the supporting protocols that were selected for evaluation in this study are:

- Connection Oriented Transport Protocol, Classes 0 through 4 (TP0, TP1, TP2, TP3, and TP4)
- Connectionless Network Protocol (CLNP)
- X.25 Packet Level Protocol
- Link Access Procedures - B (LAPB)
- Logical Link Control (LLC)
- Fiber Distributed Data Interface (FDDI)
- IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Common protocols that are excluded from this study include:

- *Upper layer security protocols (FTAM, X.400, X.509, Key Management Protocol, Security Association Management Protocol, etc.)* – these are generally associated with one application rather than a broad class of applications and services
- *Transmission Control Protocol (TCP)* – TCP is a connection oriented Transport Layer protocol that is very similar to TP4
- *Internet Protocol (IP)* – IP is a connectionless Network Layer protocol that is very similar to CLNP. (Some analysis of IP will be performed during the evaluation of addressing mode D of SP3)
- *Asynchronous Transfer Mode (ATM)* – ATM is a switching technique used to relay small cells of data over Synchronous Optical Network (SONET) channels.

Figure 1.2-1 shows the relationships of the protocols to be analyzed. The communications protocols are aligned into two primary stacks: LANs stacks, shown on the left, and WAN stacks, shown in the middle (with CLNP) and on the right (without CLNP). Each of the Network and Transport Layer security protocols, indicated by shading, will be evaluated with both types of stacks. While NLSP is shown as a Subnetwork Independent Convergence Protocol (SNICP), it can in fact be placed in any network sublayer. This is not true for SP3. The primary stacks are:

- TP4, CLNP, LLC, and a media access control protocol (CSMA/CD and FDDI will be used for this study)
- TP1, the X.25 Packet Level Protocol (with and without CLNP), and LAPB.

1.3 Study Objectives

The objectives of task 3 are to determine the extent of potential traffic flow information leakage due to the use of protocol control information that is not encapsulated when end-to-end encryption is used, and to discuss the merits of the solutions to counter those vulnerabilities.

1.4 Approach

This study was accomplished by performing the following steps:

- Discussing traffic flow confidentiality mechanisms that could be employed to reduce the vulnerability associated with traffic analysis
- Describing the characteristics of the communications and security protocols in sufficient detail to form a basis for evaluating residual traffic flow confidentiality risks when security is provided by the application process, or at the Application Layer or other layers
- Analyzing the protocol control information (PCI) in the protocol headers and trailers in order to draw inferences concerning the mission-related information that may be derived by an adversarial traffic analyst. The degree of vulnerability associated with the inferences that can be drawn by the enemy forms the basis for establishing the severity of the traffic flow confidentiality problem and the types of protective services needed from the traffic flow confidentiality mechanisms
- Analyzing the traffic flow confidentiality options and complementary combinations of options
- Recommending options to enhance security in various environments where end-to-end encryption is employed.

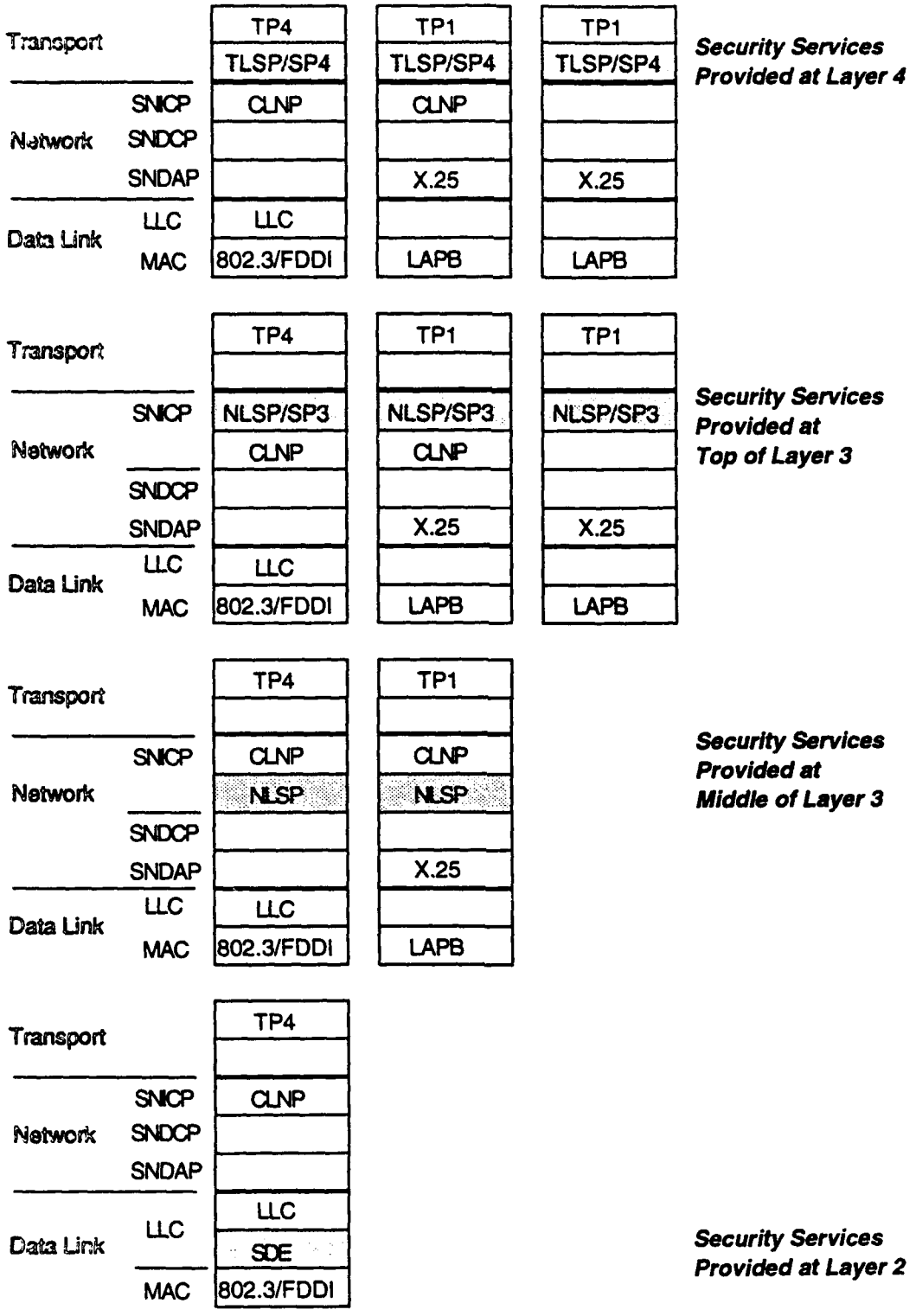


Figure 1.2-1. Protocol Stacks to be Evaluated

1.5 Report Organization

The main body of the report is organized as follows:

- **Section 1** – Introduction
- **Section 2** – Traffic Flow Confidentiality Mechanisms
- **Section 3** – Description of Protocol Characteristics
- **Section 4** – Analysis of Protocol Control Information
- **Section 5** – Analysis of Traffic Flow Confidentiality Options
- **Section 6** – Conclusions and Recommendations.

The following appendices are provided to supplement the main body:

- **Appendix A** – Acronyms
- **Appendix B** – References.

This Page Intentionally Left Blank

Section 2

Traffic Flow Confidentiality Mechanisms

This Page Intentionally Left Blank

2.0 Traffic Flow Confidentiality Mechanisms

Traffic flow confidentiality is defined in the National Information Systems Security (INFOSEC) Glossary [NSTISSI 92] as, *"Masking the frequency, length, and origin-destination patterns of communications between protocol entities in order to prevent information disclosure through inference."* The OSI Reference Model Part 2, Security Architecture Standard (ISO 7498-2) [NIST 91] defines it as, *"A confidentiality service that protects against traffic analysis."* Traffic analysis is the inference of information from observation of traffic flows (e.g., their presence, absence, amount, direction, and frequency). Traffic flow confidentiality involves security measures that prevent intruders from observing protocol control information or deriving the source or destination addresses, length of messages, time of transfer, frequency of transmission, routing policy, or other security-relevant information.

The Government Open Systems Interconnection Profile (GOSIP) [NIST 91] discusses how Federal organizations may apply the OSI Reference Model (OSI RM) (ISO 7498) to new procurements for computer networks[1]. The OSI RM Part 2, Security Architecture Standard (ISO 7498-2), addresses the traffic flow confidentiality issue. It defines traffic flow confidentiality and related terms as follows:

- **Traffic analysis** – The inference of information from observation of traffic flows (presence, absence, amount, direction and frequency).
- **Traffic flow confidentiality** – A confidentiality service to protect against traffic analysis.
- **Traffic padding** – The generation of spurious instances of communication, spurious data units and/or spurious data within data units. Traffic padding mechanisms can be used to provide various levels of protection against traffic analysis. This mechanism can be effective only if the traffic padding is protected by a confidentiality service.

The primary measure to implement traffic flow confidentiality is prevention of direct observation of information. This is accomplished with a confidentiality service, i.e., through the use of encryption for most networks or a protected distribution system for some links of a network. In addition, the ability for an adversarial traffic analyst to derive information must be prevented. This is accomplished through the insertion of dummy traffic, data padding, route control, data unit segmentation, address hiding, and timing techniques.

---

[1]GOSIP, section 4.1, states: "GOSIP does not mandate that government agencies abandon their favorite computer networking products. GOSIP does mandate that government agencies, when acquiring computer networking products, purchase OSI capabilities in addition to any other requirements, so that multi-vendor interoperability becomes a built-in feature of the government computing environment, a fact of life in conducting government business." GOSIP, section 3.2, describes a layer architecture for GOSIP that conforms to the OSI Basic Reference Model as described in ISO 7498. Therefore, while GOSIP does not explicitly require organizations to apply the OSI Reference Model, it does implicitly require its application. Future versions of GOSIP may require only that government agencies consider OSI protocol suites when acquiring computer networking products, but allow the procurement officers the latitude to actually select the protocols that best suit their needs and budget.

2.1 End-to-End Encryption

When the protocol entities that encipher and decipher data lie within hosts (or host front ends), true end-to-end encryption is provided. When one protocol entity lies in a host and the other lies in a gateway (or both lie in gateways), link encryption is provided. Of course, the path between the host and the gateway is not a link per se, but a portion of an internetwork potentially consisting of both LANs and WANs. [SSI 92]

End-to-end encryption options include determining what is to be encrypted by the protocol entity:

- The SDU or selected portions of the SDU only
- The header or selected portions of the header with the SDU
  - Full header
  - Protected Header Block (generally includes address fields, security label, integrity sequence number, and traffic padding).

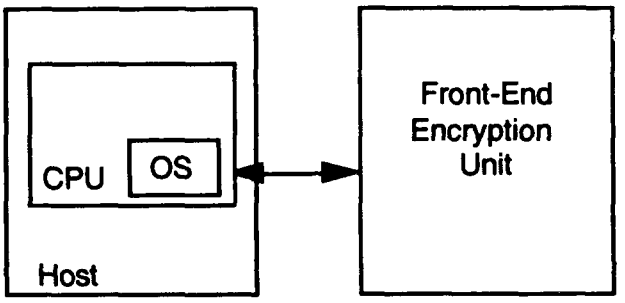
Another decision that must be made to achieve interoperable E^3 implementations is the type of encryption to be employed by the protocol entity (standards for secure protocols are usually algorithm independent):

- Symmetric – symmetric encipherment, also called *conventional encipherment,* uses an encryption algorithm and a secret key that is shared by two parties. The same key is used to decrypt the ciphertext back to plaintext. The key must be known only by the two peer entities
- Asymmetric – with asymmetric encipherment, the sender encrypts a message with the receiver's *public key* and the receiver decrypts the message using a secretly held *private key*. Public keys cannot be used to infer private keys and therefore require no protection from compromise and can be widely distributed.

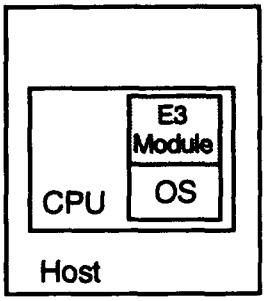
As illustrated in **Figure 2.1-1**, several options exist for providing end-to-end encryption, all of which are generally implemented in the upper layers. In figure (a), a front-end device is inserted between hosts and the network. This is the strategy being used for the BLACKER, CANEWARE, and Network Encryption System (NES) programs. A significant reduction in equipment could be effected if the end-to-end encryption system were hosted on a trusted operating system. The system could be implemented solely in software, as shown in figure (b), or could utilize a plug-in board to perform the encryption in hardware, as shown in figure (c). (Trusted systems that implement encryption solely in software are not considered to be sufficiently trustworthy for classified applications. However, such an approach could be used for sensitive unclassified applications.)

In general, end-to-end encryption options could be supported at the Presentation Layer, Transport Layer, or Network Layer. Provision of end-to-end encryption at the Presentation Layer would require that the ISO Presentation Protocol be modified through an (addendum) to support a security encapsulation function. To provide traffic

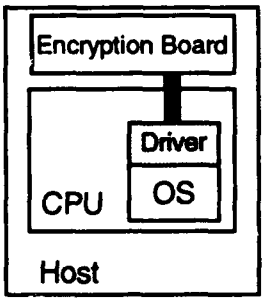
flow confidentiality, this security encapsulation function would encrypt the presentation PDUs that are created after normal Presentation Layer functions are performed. It would also be possible to implement this encapsulation function with a separate protocol entity at the bottom of the Presentation Layer (such a protocol would have to be developed). The behavior of this protocol entity would then be governed by a security protocol contained in a separate ISO standard. End-to-end encryption at the Transport Layer can be implemented with the Transport Layer Security Protocol (TLSP) or SDNS Security Protocol 4 (SP4). (Use of TLSP or SP4 always provides end-to-end encryption whenever a data confidentiality service is supported.) At the Network Layer, the Network Layer Security Protocol (NLSP) or Security Protocol 3 (SP3) both have options which provide end-to-end encryption, but can be used to provide link encryption as well.



(a) Front-End Encryption Unit



(b) Encryption Module



(c) Encryption Board

Figure 2.1-1. Options for Providing End-to-End Encryption

2.2 Link Encryption

Link encryption provides confidentiality across one physical point-to-point link between two End Systems or, more commonly, across a portion of an internetwork where one or both protocol entities lie in an Intermediate System. Link encryption can be implemented between adjacent End Systems (ES-ES), across internetworks from End Systems to Intermediate Systems (ES-IS), and between intermediate locations such as the gateways for the source and destination subnetworks, or some other intermediate points (IS-IS). Link encryption is implemented in a lower layer (Network, Data Link, or Physical). Since link encryption is implemented in a lower layer, all of the higher layer headers are protected between nodes. However, the SDUs are not protected at Intermediate Systems since they are decrypted at the end of the link. Link encryption allows Intermediate System processing of higher layer headers needed for routing and other services.

With link encryption, there is still the option of determining what is to be encrypted by the protocol entity:

- The SDU only
- The Protected Header Block with SDU.

Link encryption also offers the option of determining the type of encryption to be employed by the protocol entity: symmetric (conventional) or asymmetric (public key).

To implement link encryption at the Network Layer, NLSP or SP3 can be used. To implement link encryption on LANs, SDE can be used. Link encryption on WANs would require the development of a new security protocol. This security protocol could support bit-oriented data link protocols, such as High-level Data Link Control (HDLC), when used in point-to-point configurations. A special case of link encryption is the use of full period encryption within the physical medium. If this is done, data link frames are not distinguishable on a physical link because the physical layer adds no headers and operates on individual bits. In-line COMSEC devices, such as the KG-84A, can be used to provide link encryption at the Physical Layer.

2.3 Protected Distribution System

A protected distribution system (PDS) is a communications cable (wire or fiber optic) which includes adequate acoustic, electrical, electromagnetic, and physical (e.g., conduit and isolation) safeguards to permit it to be used for classified transmissions without the use of encryption. [NSTISSI 92] A PDS is useful in shielding the physical media of a secure network that transits a physically unsecure area. For example, a shipboard LAN that services computers in two classified areas but which includes a connecting cable that is laid in an unclassified corridor between the two areas.

2.4 Traffic Padding

Traffic padding is the basic traffic flow confidentiality countermeasure to prevent traffic analysis. It involves the generation of spurious control and information PDUs. Without traffic padding, sensitive information can be disclosed to an eavesdropper who is able to observe network traffic flows even if the individual messages are padded and encrypted. For example, the receipt of 1,000 messages per day at a military station that normally receives 100 messages may indicate that the station is involved in an important exercise or mission. If a particular mission is characterized by a unique traffic pattern, then the mission can be identified. Traffic padding can be implemented to continuously provide the same traffic flows as when the mission is actually being carried out (cover and deception). The information used to exchange network topology and delay characteristics can be used as a basis for generating dummy traffic. Traffic padding must be followed by encryption to be effective. [MUFTIC 93]

There is a negative side effect associated with traffic padding. Nodes on LANs and packet switched networks share the transmission media. If a particular route is padded to full capacity, the network cannot be shared efficiently. [FORD 94]

Traffic padding mechanisms can be implemented at the Application, Network, or Data Link Layers. To implement traffic padding at the Application Layer, an Application Service Element (ASE) could be developed which monitors traffic levels throughout the network and then internally generates dummy "control PDU" traffic and distributes it to Application Layer Specific Application Service Elements (SASEs) to cover traffic patterns. The SASEs would process this *dummy traffic* like real traffic. A variation on this approach would be to provide this functionality within the application process. The application process would transfer *dummy* data units down to the Application Layer which would then process them like real traffic.

Traffic padding mechanisms incorporated at the Network or Data Link Layers could be developed which would only be responsible for inserting dummy traffic over links. The traffic monitoring mechanisms could then rely on local information alone to control the generation of dummy traffic.

2.5 Data Padding

Data Padding extends both data and control messages to a standard size prior to encryption so that an eavesdropper cannot observe the sizes of the actual messages. If observers were able to determine actual message sizes, they might be able to infer what activity is occurring even though they cannot actually read the encrypted messages. Of course, padding is only effective when it is followed by encryption.

Data padding can be implemented in the Application Layer, Transport Layer, Network Layer, or Data Link Layer. One approach for providing this service at the application layer would be to modify application protocols associated with SASEs such as File, Transfer, Access and Management (FTAM), to pad their application PDUs to a

fixed size. This would conceal PDU sizes within an application, but not between applications. A better approach would be to develop a general-purpose ASE which provides this padding function for all Application Layer protocols.

To provide data padding at the Transport Layer, the security functions provided by TLSP or SP4 would have to be extended. NLSP provides data padding at the Network Layer, but SP3 does not if the padding field is being used to support the confidentiality or integrity encipherment algorithm, and would have to be extended. SDE would also have to be revised to support a data padding service at the Data Link Layer for LANs and MANs. A new security protocol would be required to provide data padding at the Data Link Layer for WANs.

2.6 Route Control

Route control is a mechanism which ensures that traffic is routed over gateways, subnetworks, links, and packet switches which provide adequate traffic flow confidentiality services and attributes. Routing techniques can also be used to avoid particular network components where there is a potential or known threat of passive monitoring, active wiretapping, spoofing, or jamming. For example, messages carrying certain security labels may be forbidden to pass through certain subnetworks. [MUFTIC 93] Route control can be accomplished by specifying Network Layer protection quality-of-service parameters such as security level or performance criteria, for a connection or for an individual connectionless PDU. It can also be stated explicitly using the source routing capability of Network Layer protocols.

CLNP and IP each offer two varieties of source routing: *complete* and *partial.* Complete source routing requires that the specified route be used in the exact order as shown in the route list in the PDU header. [BLACK 91] Partial source routing requires that a PDU visit all of the listed nodes but also allows a system to route PDUs to Intermediate Systems that are not specified in the list. Partial source routing is useful in forwarding traffic when the subnetwork between two Intermediate Systems is congested or out of service. Because complete source routing constrains the sequence of Intermediate Systems (and therefore subnetworks) traversed in an internetwork, it can be used as a traffic flow security mechanism. Partial source routing does not completely restrict which Intermediate Systems (and consequently which subnetworks) are traversed and is thus not employed as a traffic flow security mechanism).

Route control can be used to disperse PDUs, or PDU segments, over varied paths to prevent an adversary from accessing all of the PDUs associated with a particular session. TP4 also uses transport connection splitting to allow use of multiple network connections to provide resilience against network failure and to increase throughput. LAPB includes a multilink procedure to allow use of multiple parallel LAPB data links. The use of multiple connections or links provides a minimal level of traffic flow confidentiality when it is not possible or practical to use padding.

2.7 Segmentation

Segmentation, also called *fragmentation,* may be necessary if the size of a PDU, or derived PDU, is greater than the maximum size supported by the subnetwork or Data Link sublayer that will transmit the data. This may be necessary because of encryption or the inclusion of data padding, source routing, or other fields that enlarge the header. A segmented PDU must maintain its unique identity. [BLACK 91] Therefore, all header identifiers must be placed in the segmented PDU and are still vulnerable to traffic analysis.

Another purpose of segmentation when used with padding can be to change the size of PDUs entering and leaving a packet switch or router so that traffic flow cannot be established based on size.

2.8 Parameter Hiding

Even with the use of data padding, encryption, and segmentation, it may be possible for an eavesdropper to observe addresses and security parameters, such as priorities. Even when full SDUs are encrypted, and address and quality of service (QOS) parameters are not passed across the logical path to a peer-entity at a given layer, they are passed down to the underlying layer as parameters of the service primitive and may be incorporated into the header constructed at the next lower layer.

The only level at which complete traffic flow confidentiality can be provided is the direct-link level (e.g., Data Link and Physical Layers), because this is the only level where complete address-hiding can occur. [FORD 94] Even at the direct-link level, full address-hiding is possible only in pure point-to-point protocols (e.g., not in bus or ring LANs because multipoint protocols always convey some unprotected address information).

If the security policy prohibits the outside observation of gateway addresses and other necessary Network Layer parameters, it may be necessary to implement link encryption throughout an internetwork.

2.9 Timing Techniques

Traffic is generally sent as soon as possible because systems are designed to satisfy delivery and response time requirements within specified limits. However, when PDUs are not urgent, a traffic flow confidentiality technique is to delay some PDU transmissions to provide less accurate traffic flow information to the enemy.

2.10 Summary of Traffic Flow Confidentiality Mechanisms

Traffic flow confidentiality has been defined as a confidentiality service to protect against traffic analysis, which is the inference of information from observation of traffic flows (presence, absence, amount, direction, and frequency).

The primary measure to implement traffic flow confidentiality is the prevention of direct observation of information. This is accomplished with a confidentiality service, i.e., through the use of encryption for most networks or a protected distribution system for some links of a network. In addition, the ability for an adversarial traffic analyst to derive information must be prevented. This is accomplished through the insertion of dummy traffic, data padding, route control, data unit segmentation, address hiding, and timing techniques. The padding mechanisms must be implemented before the confidentiality mechanisms in order to be effective.

There are two options for implementing encryption: end-to-end and link encryption. When the protocol entities that encipher and decipher data lie within hosts (or host front ends), true end-to-end encryption is provided. When one entity lies in a host and the other lies in a gateway (or both lie in gateways), link encryption is provided. End-to-end encryption protects the userdata and upper layer headers from direct observation across the entire transmission path. Traffic analysis can still occur unless a padding mechanism or other service is implemented. Also, lower layer headers are not encrypted.

Link encryption protects more of the headers and reduces the ability of the traffic analyst to derive information through wiretapping. However, link encryption protects only individual links (or subnetworks) of the transmission path. An adversary who acquires access to an Intermediate System where link encryption ends could observe any upper and lower layer headers as well as userdata if they are not protected by an end-to-end encryption service as well.

An option for both end-to-end and link encryption is to determine whether the entire SDU is to be encrypted or only selected portions. Generally, security protocols encrypt selected portions while full period encryption at the Physical Layer operates on a bit stream and encrypts the entire PDU.

Another option for both end-to-end and link encryption is to determine whether to employ a symmetric (conventional) or an asymmetric (public key) algorithm.

Route control is a Network Layer mechanism which ensures that traffic is routed over gateways, subnetworks, links, and packet switches which provide adequate traffic flow confidentiality services and attributes. Routing techniques can also be used to avoid particular network components where there is a potential or known threat of passive monitoring, active wiretapping, spoofing, or jamming. Route control can also be used to disperse PDUs or PDU segments over varied paths.

Section 3

Description of Protocol Characteristics

This Page Intentionally Left Blank

3.0 Description of Protocol Characteristics

The protocols that will be analyzed can be segregated into wide area network (WAN) protocols and local area network (LAN) protocols. WANs are more complex networks than LANs, requiring several layers of protocols to provide routing, segmentation and assembly, flow control, priority processing, delivery assurance, and other services. LANs also have flow control, priority processing, and other services, although not to the same extent. LANs typically operate in a broadcast mode where all hosts monitor the line and ignore what is not addressed to them. The WAN-oriented protocols described in **Section 3.1** are:

- ISO 8073 Connection Oriented Transport Protocol (TP0, TP1, TP2, TP3, and TP4) [ISO 88]
- ISO 10736 Transport Layer Security Protocol (TLSP) [ISO 92A and 92C]
- NSA Secure Data Network System (SDNS) Security Protocol 4 (SP4) [NIST 90]
- ISO 8473-1 Connectionless Network Protocol (CLNP) [ISO 92D]
- ISO 11577 Network Layer Security Protocol (NLSP) [ISO 92B]
- NSA SDNS Security Protocol 3 (SP3) [NIST 90]
- ISO 8208 – X.25 Packet Layer Protocol [ISO 90C]
- CCITT Link Access Procedures - B (LAPB). [CCITT 88]

The LAN-oriented protocols described in **Section 3.2** are:

- ISO 8802-2 Logical Link Control (LLC) [ISO 90B]
- IEEE 802.10 Secure Data Exchange Protocol (SDE) [IEEE 93A]
- ISO 9314 Fiber Distributed Data Interface (FDDI) [ISO 89B, 89C, and 90A]
- ISO 8802-3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD). [ISO 93]

A protocol entity operating at a given layer on a source network component communicates with the protocol entity at a corresponding layer on the destination component. This peer-to-peer communication is accomplished using *protocol data units* (PDUs). PDUs in the Data Link Layer are commonly referred to as *frames*, and PDUs in the Network Layer are sometimes referred to as *packets*. Each layer uses the services provided by the layer below it in order to deliver the PDUs to its corresponding peer entity.

Interactions between adjacent layers are managed by exchanging messages called *service primitives.* [SPRAGINS 92] Service primitives are divided into four different categories to reflect whether they are used on a source or destination network

component, and whether they are going up or down across the layer boundary. The four categories of service primitives, illustrated in **Figure 3-0.1**, are:

- **request** – service primitive goes down from service user to the service provider on source component; allows service user to make a request for some network service
- **indication** – service primitive goes up from service provider to service user on destination component; informs destination about service request
- **response** – service primitive goes down from service user to the service provider on destination component; returns response to source if required
- **confirm** – service primitive goes up from service provider to service user on source component; informs source about status of request. [SSI 92]

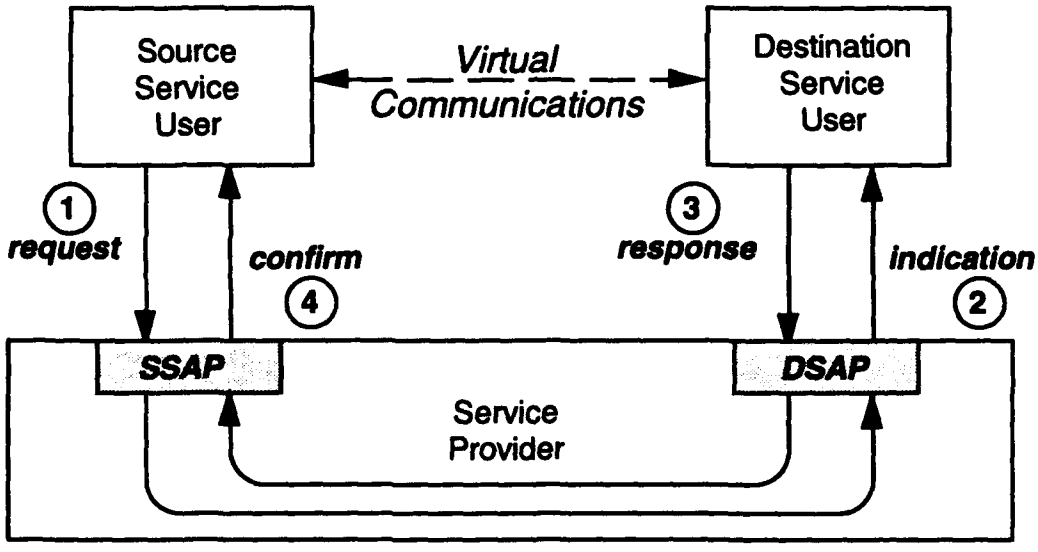


Figure 3.0-1. Relationships Among Service Primitive Categories

In a *confirmed service,* all four of these service primitive types are used in the following sequence: **request, indication, response,** and **confirm**. Data is therefore exchanged in both directions between the protocol entities to provide an acknowledgment to the sender. In an *unconfirmed service,* only the first two primitives are used. Data is thus sent from the source to the destination entity without a return path, and thus with no mechanism for the receiver to return an acknowledgment to the sender. The CONNECT service primitive in a connection-oriented protocol is an example of a primitive that is always confirmed because the remote peer must agree to establish the connection. Data transfers, on the other hand, can be either confirmed or unconfirmed. An unconfirmed service allows data transfers with a minimum of protocol

overhead. Connectionless protocols generally provide unacknowledged service and simply discard PDUs that are found to contain transmission errors. Retransmission, a function of error recovery and sequencing, is the responsibility of a higher protocol layer.

One convention for representing service primitives is to begin them with a name that captures the essence of the service requested (e.g., connection-oriented CONNECT, SYNCHRONIZE, EXPEDITED_DATA, DATA, EXCEPTION_REPORT, INTERRUPT, RESET, DISCONNECT, and other primitives, and connectionless UNITDATA primitives), followed by the specific type of service primitive represented (request, indication, response, or confirm).

For example, one basic service provided by many layers is to establish a connection between two entities (CONNECT). This is a confirmed service that uses the following service primitives:

- CONNECT.request
- CONNECT.indication
- CONNECT.response
- CONNECT.confirm.

Release of a connection (DISCONNECT) is an example of an unconfirmed service. The connectionless UNITDATA is another example. The DISCONNECT PDU uses the following service primitives:

- DISCONNECT.request
- DISCONNECT.indication.

Another convention is to prefix service primitives with abbreviations for the layers they operate at. For example, a CONNECT.request is called DL_CONNECT.request at the Data Link Layer and N_CONNECT.request at the Network Layer. Commonly used abbreviations for the other layers and sublayers are: A for Application Layer, P for Presentation Layer, S for Session Layer, T for Transport Layer, SN for Subnetwork, UN for Underlying Network, MA for Media Access Control Sublayer of the Data Link Layer, and PH for Physical Layer.

Each primitive contains parameters such as calling address, called address, QOS, and userdata. The userdata parameter is actually the Service Data Unit (i.e., PDU with its protocol header) passed down from the layer above. As a service provider to the layer above, each layer offers a variety of QOS options that can be selected by the service user (i.e., the layer above) that collectively specify the performance of the service being provided. Examples of QOS parameters are: *throughput* expressed as the number of octets or bits successfully delivered within a specified period; expected *transit delay* from the source to the destination; *residual error rate* which defines the number of lost, duplicated, or incorrectly delivered service data units as a percentage of the total transmitted; relative *priority* of the service data unit; *resilience* which is the probability of a non-orderly release of the connection; *protection*, defined as the extent

to which the service provider will attempt to prevent unauthorized monitoring or manipulation of the data; *flow control; segmentation* permitted; and others. **Figure 3.0-2** identifies the common parameters that are made available by a service provider to the service user in the Open Systems Interconnection (OSI) architecture. The Application Layer is not shown because each application provides a unique set of parameters with little commonality.

For example, while looking at **Figures 1.1-1** and **3.0-2**, assume that an application process wishes to transmit some data to a corresponding application process on the remote host. The application process will request communication service from the Application Layer. That request consists of several parameters, including the source and destination addresses, application QOS parameters, and the application data. To service the request, the Application Layer protocol entity will send an A_CONNECT PDU to the corresponding Application Layer protocol entity on the remote host to establish a connection.

To send the A_CONNECT PDU, the Application Layer will request communication service from the Presentation Layer through an address known as a Service Access Point (SAP). The service request consists of a primitive with several parameters, including the calling and called addresses (i.e., the presentation source and destination SAPs), presentation quality of service parameters, a serial number, and the presentation service data unit (SDU, i.e., the application PDU with its application header). To service that request, the Presentation Layer protocol entity will send a P_CONNECT PDU to the corresponding Presentation Layer protocol entity on the remote host to establish a connection.

To send the P_CONNECT PDU, the Presentation Layer will request communication service from the Session Layer. The request consists of several parameters, including the calling and called addresses (i.e., Session SSAP and DSAP), session quality of service parameters, a serial number, and the session SDU (i.e., the presentation PDU with its presentation header). To service that request, the Session Layer protocol entity will send an S_CONNECT PDU to the corresponding Session Layer protocol entity on the remote host to establish a connection.

The Session Layer will repeat the process by requesting communication service from the Transport Layer. The Session Layer has the choice of selecting connection-oriented or connectionless transport service. This choice is identified by the address parameters (e.g., the Transport SSAP and DSAP) that are used in the request. In general, a protocol entity within a layer can be attached to one or more SAPs at the upper layer boundary and lower layer boundary. An individual SAP can only be attached to one entity above the layer boundary and one entity below the layer boundary at any time. The appropriate Transport Layer protocol entity will then service the request by transmitting a T_UNITDATA PDU or a T_CONNECT PDU, depending on whether the selected protocol provides connectionless or connection-oriented service.

The Transport Layer protocol entity, whether it is connection-oriented or connectionless, will request communication service from the Network Layer. Again, the

Transport Layer protocol entity has the option of selecting connection-oriented or connectionless network service. The process repeats for each layer until peer-to-peer connections are established or connectionless protocols have been selected at each layer. *The important point is that primitives and their associated parameters are passed up and down across layer interfaces on the same network component while PDUs are actually transmitted between the components that support the peer-entities. But there must be enough information (including security-relevant information) in the PDU for a protocol entity on an intermediate or destination system to pass parameters back up to the layer above.*

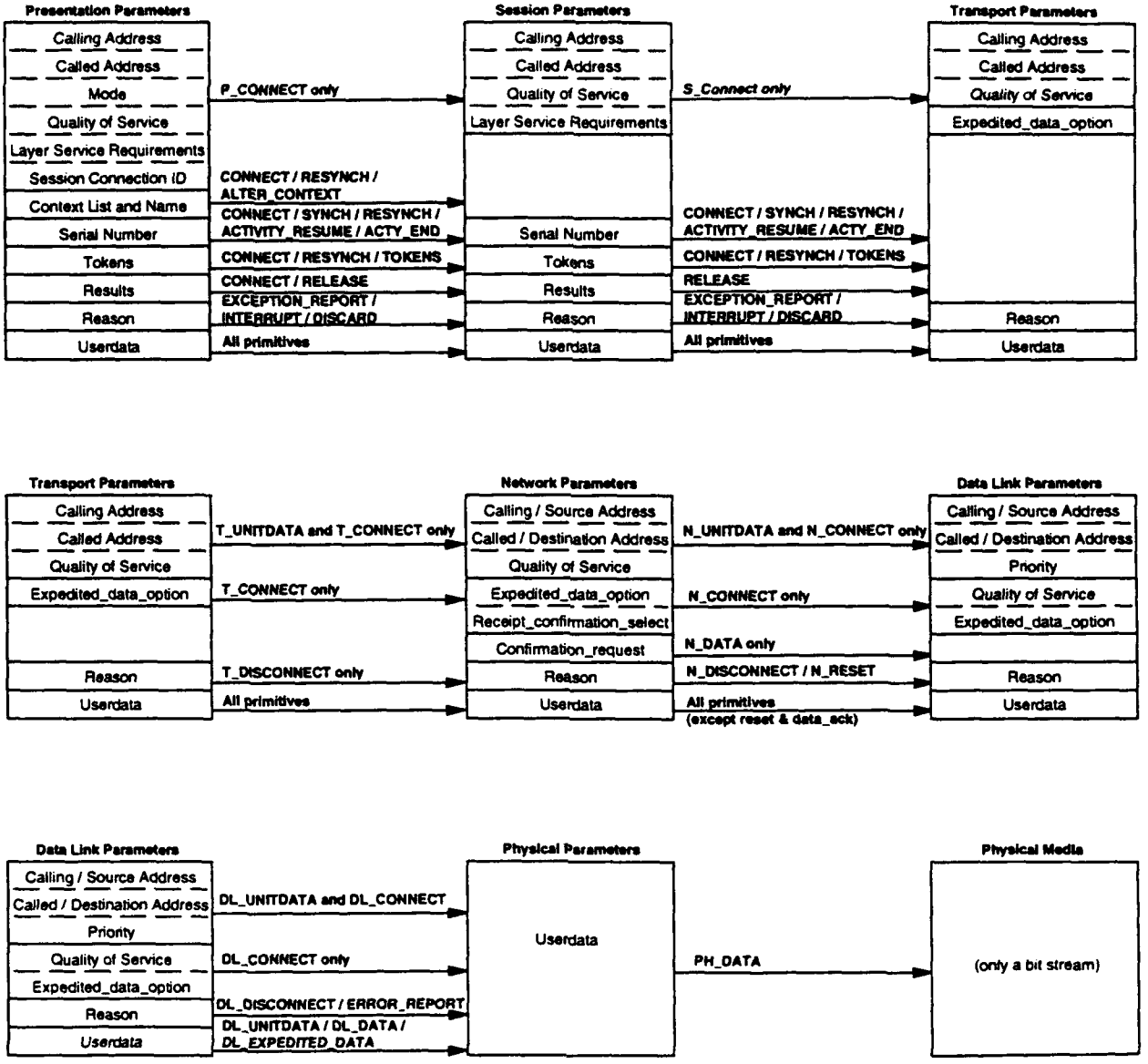


Figure 3.0-2. Primitives and Parameters Provided in the OSI Architecture

As indicated, there are two basic types of protocols: connection-oriented and connectionless. Connection-oriented protocols expend overhead by transmitting extra PDUs to establish an end-to-end connection, then save overhead associated with each DATA PDU by not including address and service parameters. Connectionless protocols save overhead by not sending CONNECT PDUs to establish a connection, then expend overhead by including necessary control information with each UNITDATA PDU. Connection-oriented protocols have been referred to as being similar to the telephone system where a caller must first establish an end-to-end connection prior to initiating communications. Connectionless protocols have been referred to as being similar to the postal system where messages can be sent without establishing a connection, but where each message requires routing and handling instructions. For large file transfers, connection-oriented communications is preferable. For short messages such as electronic mail or remote terminal activity, connectionless communications is more efficient.

Connection-oriented and connectionless protocols are compatible in the same protocol stack. In other words, a connection-oriented protocol may be used at the Transport Layer while a connectionless protocol provides the required services at the Network Layer. In fact, it is very common to see a connection-oriented transport protocol being supported by a connectionless network protocol, which is in turn supported by a connection-oriented data link protocol. The security protocols designed for Layers 2, 3, and 4 all operate with both connection-oriented and connectionless protocols.

The Institute of Electrical and Electronics Engineers (IEEE) Project 802 Working Group developed a family of standards that divides the Data Link Layer into the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) Sublayer. The parameters passed by these sublayers are shown in **Figure 3.0-3**.

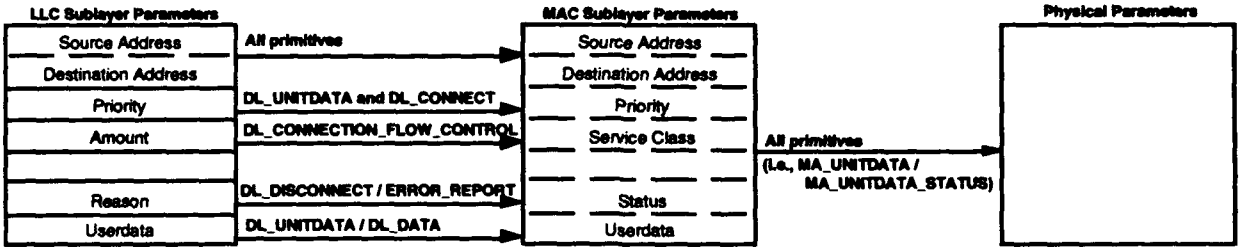


Figure 3.0-3. Primitives and Parameters Provided in the IEEE Architecture

3.1 WAN Protocol Descriptions

The following WAN-oriented generic communications protocols and security protocols are described in this section:

- Connection Oriented Transport Protocol (TP0, TP1, TP2, TP3, and TP4)
- Transport Layer Security Protocol (TLSP)
- SDNS Security Protocol 4 (SP4)
- Connectionless Network Protocol (CLNP)
- Network Layer Security Protocol (NLSP)
- SDNS Security Protocol 3 (SP3)
- X.25 Packet Level Protocol
- CCITT Link Access Procedures - B (LAPB). [CCITT 88]

The descriptions of these protocols are accompanied by graphics that depict the fields in the protocol data units, and the security association attributes contained in the peer Security Management Information Base (SMIB). Each figure contains a number of abbreviations which are defined in **Table 3.1-1**.

Table 3.1-1. *Abbreviations*

Abbreviation	Definition	Abbreviation	Definition
AK	Acknowledgement	MDF	Management defined field
ASSR	Agreed set of security rules	MSDU	MAC service data unit
CL	Connectionless	NSAP	Network service access point
CLNPHDR	CLNP header	NSDU	Network service data unit
CO	Connection-oriented	PAD	Padding field
CR/CC	Connect request/confirm	PE	Peer-entity (authentication)
DO	Data origin (authentication)	P/F	Poll/final bit
DSAP	Destination SAP	PID	Protocol ID
DT	Data PDU	QOS	Quality of service
ED	Expedited data PDU	SA	Security association
EKE	Exponential key exchange	SAID, SA-ID	Security association ID
EOT	End of TSDU mark	SDT	Secure data transfer
ER	Error PDU	SE TPDU	Security encapsulation TPDU
ES	End System	SMIB	Security management information base
FCS	Frame check sequence		
ICV	Integrity check value	SMT	Station management (FDDI)
I/G	Individual/group bit	SSAP	Source service access point
IPHDR	IP header	TPDU	Transport protocol data unit
ISN	Integrity sequence number	U/L	Universal/local bit

3.1.1 Description of Connection Oriented Transport Protocol, Classes 0 through 4 (TP0, TP1, TP2, TP3, and TP4)

The Connection Oriented Transport Protocol (ISO 8073) [ISO 88], shown in **Figure 3.1-1**, is the primary protocol provided at Layer 4. It offers five classes of service and is useful with all types of network connections. ISO 8073 defines three types of networks: 1) high quality (Type A) networks provide acceptable residual failure rates and acceptable rates of signaled errors so that packets can be assumed not to be lost, and the Transport Layer need not provide recovery or resequencing; 2) medium quality (Type B) networks provide for acceptable residual error rates, but unacceptable signal failure rates, so the Transport Layer must be able to recover from failures; and 3) low quality (Type C) networks provide an unacceptable residual error rate such that the Transport Layer must be able to both recover from failures and resequence packets.

Classes 0 and 2 (simple class and multiplexing class, respectively) are designed for use over high quality network connections. Classes 1 and 3 (basic error recovery class and multiplexing with basic error recovery class, respectively) are designed for use over medium quality network connections. Class 4 (error detection and recovery class) is designed for use over low quality network connections. This study will primarily consider TP1 and TP4 because these are the most commonly used classes in implemented systems. TP1 is generally used with network protocols that reset, clear, and restart with unacceptable rates of data loss, such as X.25. TP4 is generally used with connectionless network protocols which can lose or reorder PDUs, or deliver PDUs with undetected errors, such as CLNP.

TP1 provides acknowledgment and reject functions while TP4 provides multiplexing, explicit flow control, checksumming, frozen references, retransmission on timeout to cope with unsignalled TPDU loss by the network service provider, resequencing to cope with TPDU misordering by the network service provider, inactivity control to cope with unsignalled network connection termination, and PDU splitting to allow simultaneous use of multiple network connections. Both classes allow concatenation of multiple TPDUs into one NSDU. Class 4 does not provide a reject PDU function.

As shown in **Figure 3.1-1**, PDU types are CONNECT and DISCONNECT, DATA and EXPEDITED_DATA, ERROR, DATA_ACK, and REJECT. PDUs consist of a length indicator field, a Fixed Part, a Variable Part, and Unitdata (e.g., the Service Data Unit from the Session Layer). The Fixed Part is present in all PDUs and consists of frequently occurring parameters such as connection references, peer sequence numbers (ACK and REJECT PDUs), and reason (DISCONNECT and ERROR PDUs).

The Variable Part consist of less frequently occurring parameters such as quality of service parameters and checksum. Userdata can be passed in the DATA PDU and in CONNECT and DISCONNECT PDUs by both TP1 and TP4.

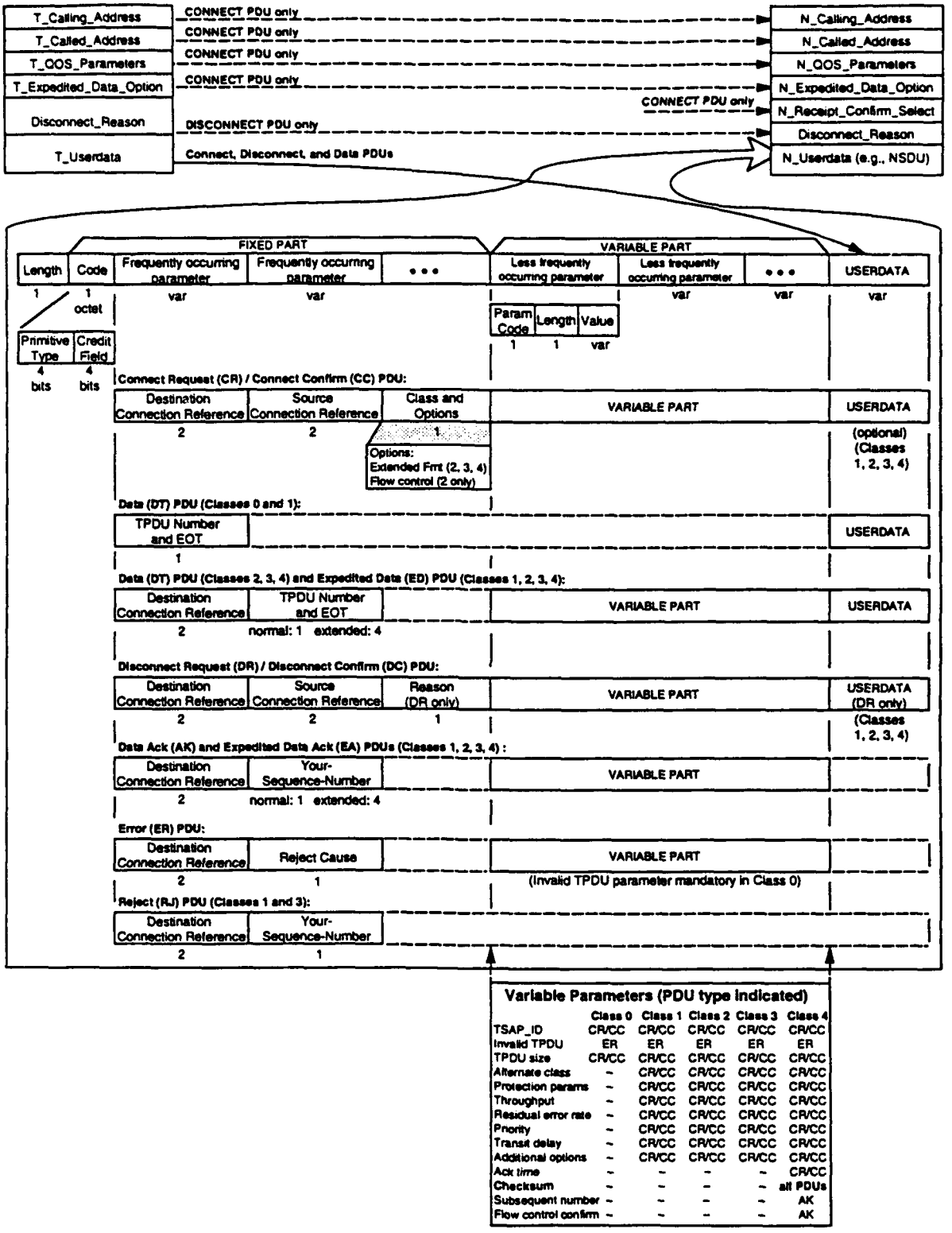


Figure 3.1-1. Connection Oriented Transport Protocol (COTP) Protocol Data Units

3.1.2 Description of Transport Layer Security Protocol (TLSP)

The Transport Layer Security Protocol (ISO 10736) [ISO 92A and 92C] is designed to provide optional end-to-end integrity, confidentiality, authentication, and access control functions that extend the capabilities of the Connection Oriented Transport Protocol (ISO 8073) and the Connectionless-Mode Transport Protocol (ISO 8602). TLSP encapsulates Transport PDUs in a security envelope using encryption, an integrity check value, or both and passes the PDU and other parameters to the underlying layer, as shown in **Figure 3.1-2**. It also provides security labeling which supports mandatory access control mechanisms.

Implementation of TLSP on a host does not preclude the use of unprotected communications between transport protocol entities because the formats of all parameters sent down from the Transport Layer communications protocol are preserved and passed to the Network Layer. While the formats are preserved, the actual address parameter values are amended to indicate the SAPs for the TLSP protocol entities. QOS and Userdata parameters are also amended but their formats are preserved.

In addition to the Security Encapsulation PDU, TLSP defines a Security Association PDU that is used to establish a security association (SA) between corresponding TLSP protocol entities, establish confidentiality and integrity keys, initialize integrity sequence numbers for the SA, rekey when a key is about to expire, define security labels for the SA, and define security QOS values for the SA. Key management can be controlled internally by TLSP or externally by a key management protocol operating at Layer 7. In either case, security association attributes are maintained by both peer-entities in their respective Security Management Information Bases (SMIBs). These attributes are accessible by system management, security management, and key management protocols. They are referenced by a Security Association Identifier (SA-ID) field in the TLSP Security Encapsulation PDU.

3.1.3 Description of SDNS Security Protocol 4 (SP4)

Security Protocol 4 (SP4) is one of the four Secure Data Network System (SDNS) protocols. [NIST 90] SP4 operates with both connection-oriented and connectionless transport protocols and does not preclude the use of unprotected communications. Therefore, SP4-capable hosts can operate in networks where not all stations use SP4 and can communicate with both protected and unprotected hosts if that is allowed by the local security policy. SP4 performs security labeling and Transport PDU encapsulation using encryption and integrity check values in the same manner as TLSP.

One distinction between SP4 and TLSP is that SP4 allows for the use of a Final Sequence Number (FSN) to detect truncation (the deletion of the PDUs transmitted at the end of a transport connection). The FSN field conveys the sequence numbers of the last PDUs sent and transmitted over the transport connection so that both sides can determine if all PDUs have been received.

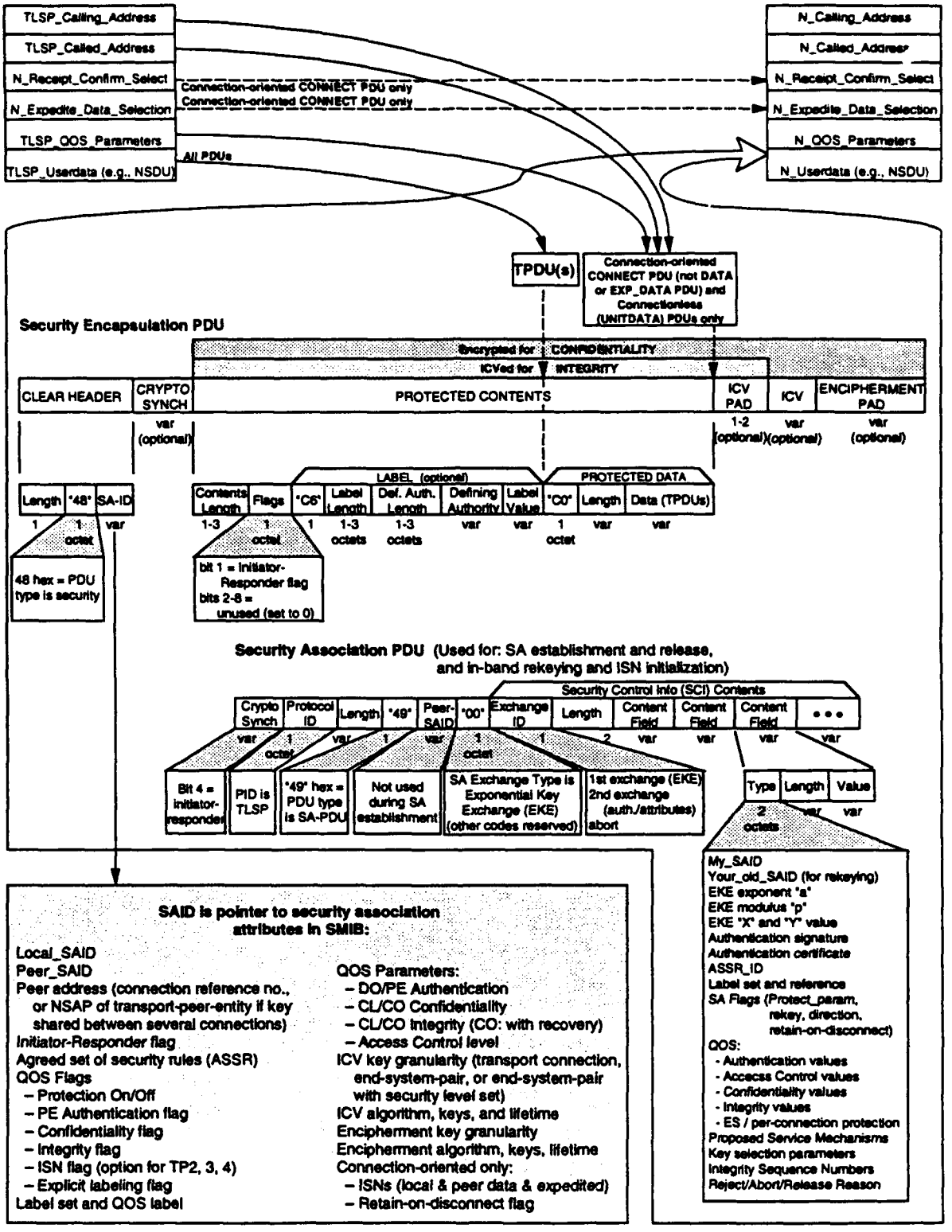


Figure 3.1-2. Transport Layer Security Protocol (TLSP) Protocol Data Units

Unlike TLSP which incorporates internal key management functions, SP4 has no security association PDU and must rely on different security protocols within the stack for SA establishment (external key management protocols). The SDNS Key Management Protocol (KMP) has been specifically designed to create security associations for SP4.

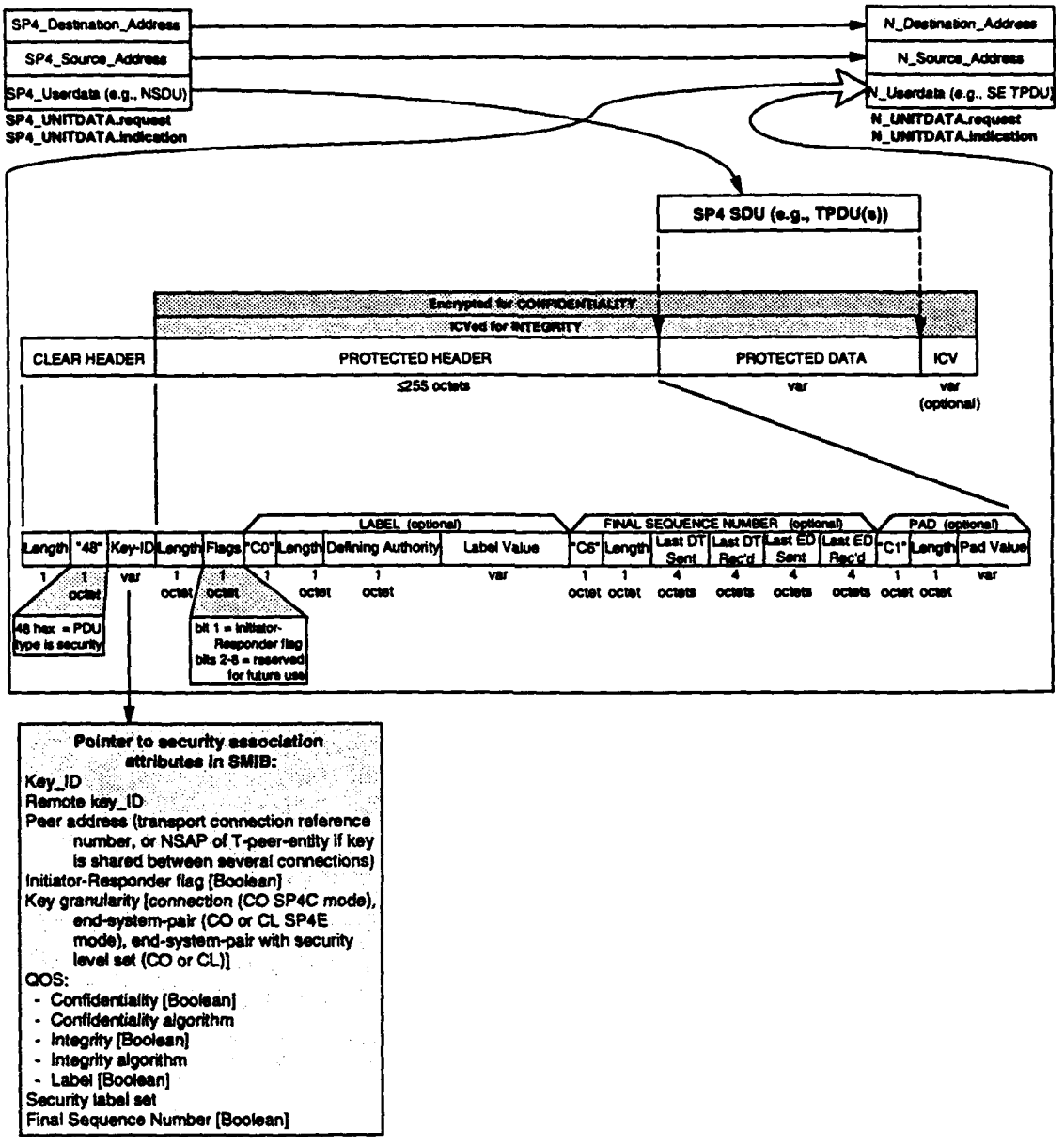


Figure 3.1-3. SDNS Security Protocol 4 (SP4) Protocol Data Unit

3.1.4 Description of Connectionless Network Protocol (CLNP)

Connectionless Network Protocol (CLNP) (ISO 8473-1) [ISO 92D] functions include PDU segmentation and assembly, source routing, route recording, security level (label), prioritization, network congestion notification, error reporting, and PDU lifetime control (i.e., expiration counter). CLNP is a Subnetwork Independent Convergence Protocol (SNICP) that may be used between Network Layer peer-entities in Intermediate Systems (IS), in End Systems (ES), or in both. (A SNICP provides relay and routing services for internetworking, one of the three major functions of the Network Layer. The other two major functions are the Subnetwork Dependent Convergence Function, which brings the interconnecting networks up to a level needed for the interconnection, and Subnetwork Access Function, which contains the services relevant to an interconnecting network.) CLNP relies upon an underlying connectionless service provided by real subnetworks or data links. The underlying service may be obtained either directly, from a real connectionless subnetwork or data link such as ISO 8802-2 Logical Link Control (LLC), or indirectly from a Subnetwork Dependent Convergence Protocol (SNDCP) operating over a real connection-oriented subnetwork such as X.25 Packet Level Protocol.

The CLNP PDU, shown in **Figure 3.1-4**, consists of a Fixed Part, Address Part, Segmentation Part, Options Part, and Data Part. The Fixed Part and Address Part are mandatory while the Segmentation, Options, and Data Parts are optional. The checksum is calculated for the entire CLNP header to include all parts except the Data Part and all fields except the Checksum Field itself. The PDU parameters field indicates whether the PDU is a Data PDU or an Error Report PDU. The Segmentation Part is present when a Data PDU is segmented in order to meet size limitations of the underlying subnetwork.

CLNP Options include padding to meet transmission size requirements, source routing that allows the originating ES to determine the route of the PDU, route recording which is intended to provide a return path for subsequent PDUs and to support diagnosis of subnetwork problems, quality of service (QOS) values that can be used by IS network protocol entities to make routing decisions, a congestion flag that can be set by any IS to inform the destination network protocol entity that congestion exists on the path traversed by the PDU, a priority value for expedited processing, and security. The priority function provides a means whereby transmission queues and buffers and other resources can be used to process higher-priority PDUs ahead of lower-priority PDUs. ISO 8473-1 states that implementation specifics are a local matter. Therefore, this option could be used by DoD system designers to implement processing according to DoD communications priorities (i.e., Routine, Priority, Immediate, Flash, and Flash Override). The security option includes data confidentiality and data integrity provided via route control, and data origin authentication provided via a cryptographically generated or enciphered checksum that is separate from the PDU Header checksum. While these security services are covered in the CLNP standard, it is doubtful they will ever be implemented due to the emergence of NLSP.

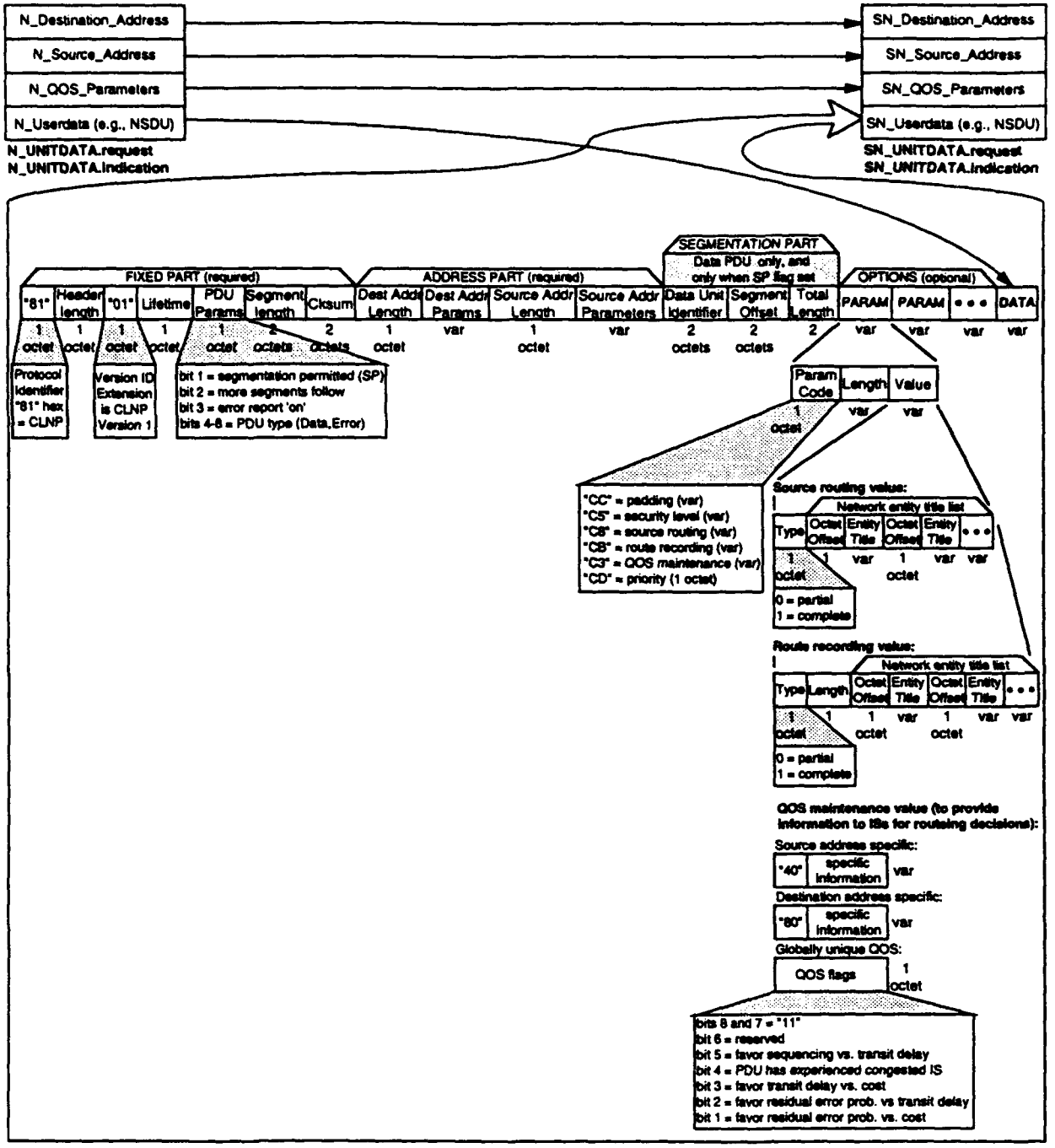


Figure 3.1-4. Connectionless Network Protocol (CLNP) Protocol Data Unit

3.1.5 Description of Network Layer Security Protocol (NLSP)

The Network Layer Security Protocol (ISO 11577) [ISO 92B], shown in **Figure 3.1-5**, is designed to extend the capabilities of both connection-oriented and connectionless network protocols by encapsulating Network PDUs in a security envelope using encryption, an integrity check value, or both, and by providing security labeling. NLSP can operate at various subnetwork layers. It can provide connectionless end-to-end security services by operating as a SNICP on top of CLNP at the top of Layer 3. It can also provide connectionless link security services by operating below CLNP. For connection mode communications, NLSP operates above a SNICP or subnetwork access protocol such as X.25. NLSP does not preclude the use of unprotected communications between network protocol entities. Therefore, NLSP-capable hosts can operate in networks where not all stations use NLSP and can communicate with both protected and unprotected hosts if that is allowed by the local security policy.

NLSP defines three PDU types: a Security Association PDU that is used to establish a security association (SA) between corresponding NLSP entities, a Secure Data Transfer PDU that encapsulates Network SDUs, and a Connection Security Control PDU that establishes cryptographic and integrity keys, initializes integrity sequence numbers (ISNs) for the SA, and reestablishes keys when a key is about to expire. Key management can be controlled by NLSP or externally by a Layer 7 key management protocol. In either case, security association attributes are maintained by both peer-entities in their respective SMIBs, and are referenced by the SA-ID field in the Unprotected Header.

NLSP provides traffic padding for traffic flow confidentiality in addition to padding needed to support the block integrity and encipherment algorithms. CLNP source routing and route recording capabilities will be preserved when NLSP operates above CLNP to provide end-to-end security. This arrangement can only be used between two End Systems. When NLSP is operated below CLNP, source routing and route recording become NLSP QOS parameters. An alternative is to provide CLNP sublayers both above and below NLSP. This stack is the most flexible. The upper CLNP would provide complete internetwork routing, NLSP would connect "trusted" relays, and the lower CLNP protocol would provide routing across the "untrusted" domain.

NLSP also provides an option for address hiding. When this is selected, the addresses used at the underlying network service interface are those of the NLSP entities (which may lie within an Intermediate or End System) rather than the Network Service Access Point addresses or the Subnetwork Point of Attachment addresses (depending on whether the system is designed with NLSP implemented at the top of Layer 3 or under another network protocol such as CLNP, respectively).

For connection-oriented communications only, NLSP can provide additional traffic flow confidentiality by hiding the NLSP address through the use of a No_Header encapsulation option. However, with the No_Header option, the security label, ICV, ISN, and padding cannot be used. If such security functions are required, then it is still

possible to use the NLSP No_Header encapsulation option by providing these functions at higher layers or within the application process itself. For example, a label can be applied by the Transport Layer, Application Layer, or application process. Padding for traffic flow confidentiality can be applied by the application process or by an Application Layer protocol. If the encryption algorithm used with the No_Header encapsulation option provides error extension, a higher layer protocol with linear error detecting code (such as TP4) can provide a secure connectionless integrity service. If the sequence numbers in a higher layer protocol (such as TP4) are protected against unauthorized modification by the connectionless integrity service, then connection integrity can also be provided.

3.1.6 Description of SDNS Security Protocol 3 (SP3)

SDNS Security Protocol 3 (SP3) [NIST 90] performs connectionless network security labeling, access control (based on the label and network service access points), and Network SDU encapsulation using encryption and integrity check values. SP3 assumes it is operating over a connectionless network service, such as CLNP or IP, but can also operate below these protocols if the system architects choose to implement it that way. It operates end-to-end, ES-to-IS, or IS-to-IS, and does not preclude the use of unprotected communications between a system which has SP3 and a system that does not. (The use of such features for classified applications requires a trustworthy architecture to avoid an unauthorized bypass of security services.) SP3 has no security association PDU and must rely on external key management protocols for SA establishment. The Key-ID field references the traffic encryption key (TEK) and associated security attributes that are maintained in the SMIBs on both hosts for the SP3 peer entities.

SP3 operates as a SNICP at the top of Layer 3 in any of four addressing modes: no addresses (SP3N), addresses in the header (SP3A), header includes an ISO CLNP header as a protected field (SP3I), and header includes a DoD IP header as a protected field (SP3D). When a host wants to establish an SP3 security association with another host so that they can communicate securely, it specifies the addressing mode that it wants to use for the session. It the remote host is not SP3-capable but is connected to a secure subnetwork, the source host could establish an SP3 security association with the gateway to the remote host's secure subnetwork. SP3N addressing mode, shown in **Figure 3.1-6**, is only used end-to-end. In this mode, the address parameters received in the UNITDATA.request are passed through as parameters in the N_UNITDATA.request to the network sublayer below. In addressing modes SP3I and SP3D, the QOS parameters are encapsulated in the CLNP or IP header. Construction of the CLNP or IP headers can include source routing and route recording address parameters.

NSA has indicated their intention to upgrade SP3 to accommodate connection-oriented network protocols in the future. However, NLSP is emerging as a preferred protocol due to its status as an International Standard. Furthermore, NSA has announced that it plans to add NLSP to SDNS. Therefore, SP3 may never be upgraded and may eventually be abandoned.

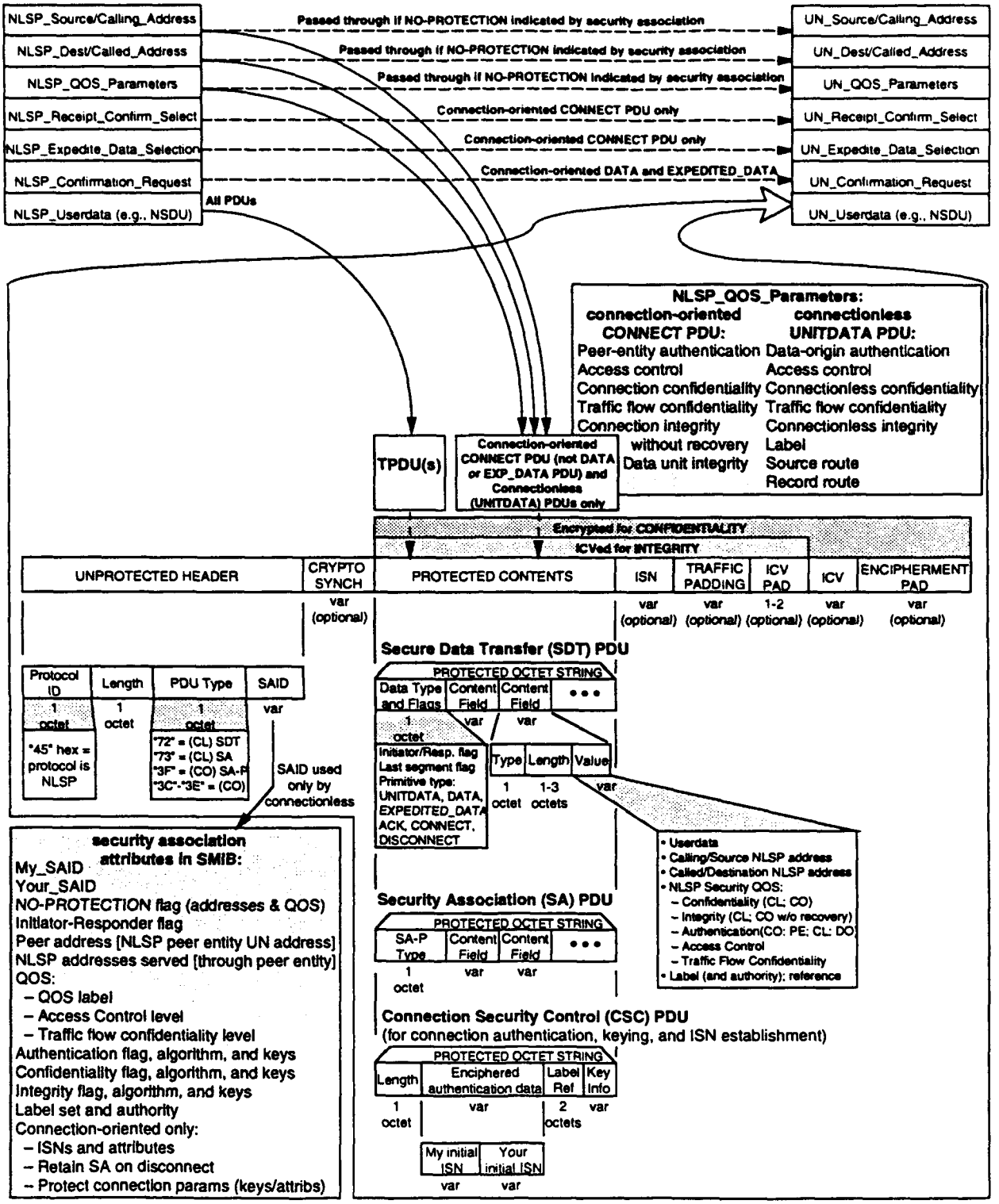


Figure 3.1-5. Network Layer Security Protocol (NLSP) Protocol Data Units

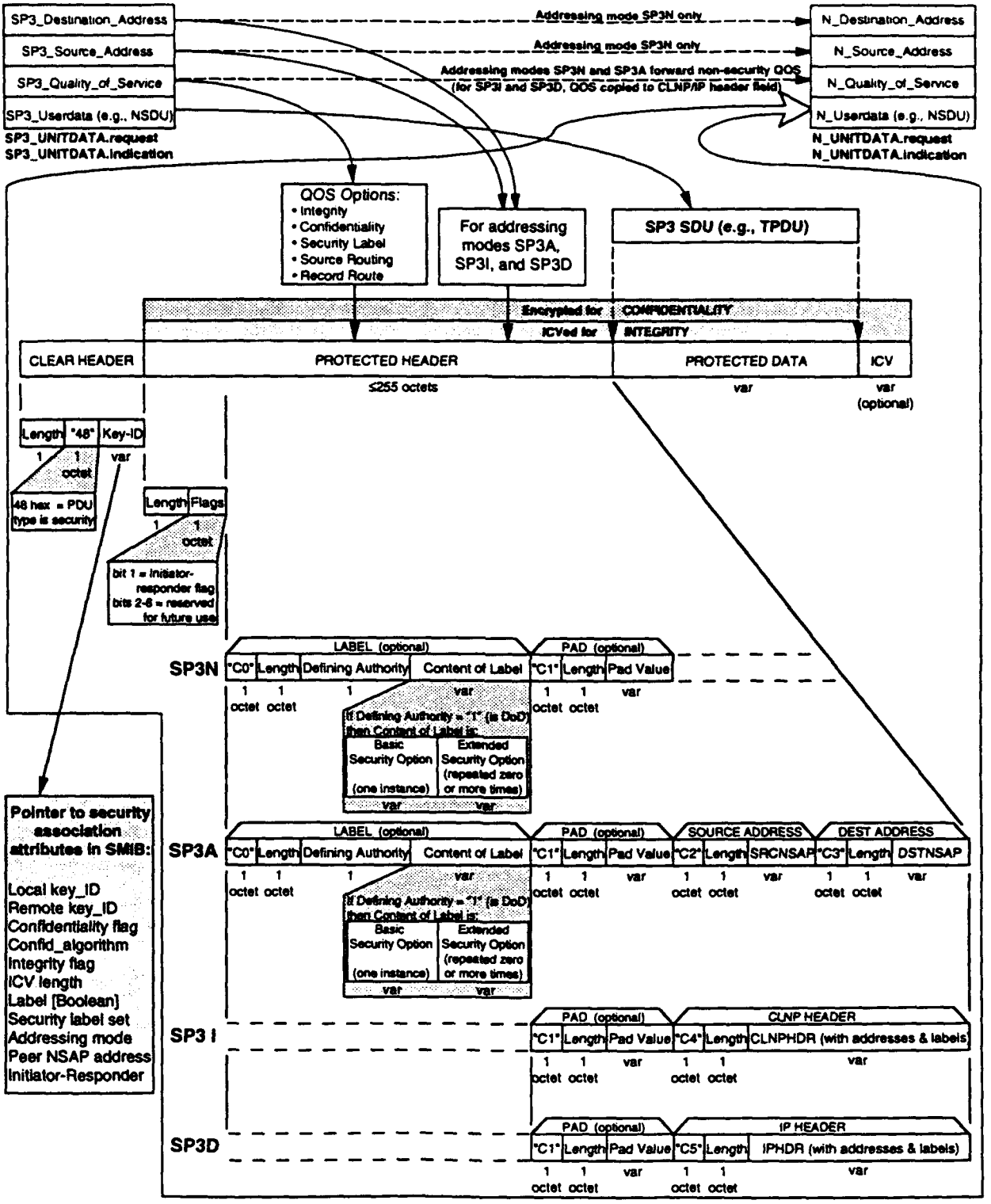


Figure 3.1-6. SDNS Security Protocol 3 (SP3) Protocol Data Units

3.1.7 Description of X.25 Packet Level Protocol

The X.25 Packet Level Protocol (ISO 8208) [ISO 90C] (commonly known as CCITT Recommendation X.25) [CCITT 88] provides specifications for packet-mode switching to furnish connection-oriented WAN connectivity — virtual circuits (vice connectionless connectivity by CLNP and LAN stack protocols). The Packet Layer provides two types of virtual circuit service to the Network Sublayer or Transport Layer above: *virtual calls* that are comparable to dial telephone calls that require connect and disconnect phases, and *permanent virtual circuits* that are permanently set up between source and destination. [SPRAGINS 92] Virtual circuits are collections of individual logical point-to-point connections identified by unique Logical Channel Numbers (LCNs). After Call Setup, data packets flowing over the X.25 DTE/DCE interface contain the LCN rather than network addresses.

Packet switching segments connection-oriented messages into small packets, appends the destination address or LCN and sequence number to each packet, transmits the packets across diverse routes on the network, and reassembles the packets into their original order at the destination node. [SCHLAR 90] In some cases, this approach provides better security than circuit switched communications because interception of the packets on one channel may yield only part of the message. Transmission is faster than with message switching because the small packets are processed faster by the network. However, packet switching creates additional traffic on the network because it requires Call Setup and Clear phases where message switching needs only a data transfer phase.

CCITT Recommendation X.25 contains specifications for the X.25 Packet Level Protocol at Layer 3, LAPB at Layer 2, and X.21 bis at Layer 1. **Figure 3.1-7** shows the X.25 Layer 3 PDUs. All PDUs have a General Block which contains format, Logical Group Number (LGN), and LCN fields. A registration request is used by a DTE (Data Terminal Equipment, e.g., source host) to establish or discontinue an agreement with a DCE (Data Circuit-terminating Equipment, e.g., network connection point) for use of an optional user facility (e.g., fast select, extended sequencing, flow control, packet and window sizes, closed user groups, one-way logical channels, etc.).

There are four major categories of communications packets: Call Setup/Clear, Data/Interrupt, Flow Control, and Reset/Restart. There is also a diagnostics packet, not discussed in this report. The Call Setup phase begins with a source DTE transmitting a Call Request. This transforms into an Incoming Call being transmitted from the DCE to the destination DTE. The destination responds with Call Accepted, which is returned by the DCE to the source DTE as Call Connected. These PDUs include calling and called DTE addresses, optional user facility selections, and optional data.

Data PDUs follow with no address block. However, they do contain the LCN and also contain send and receive sequence numbers for reassembly. (Note: the order of the sequence numbering fields has been simplified in the figure, and there is a one-bit "zero" field not shown.) Flow control PDUs are used to throttle the data between the DTE and DCE to ensure that the sender transmits Data packets at a rate that the

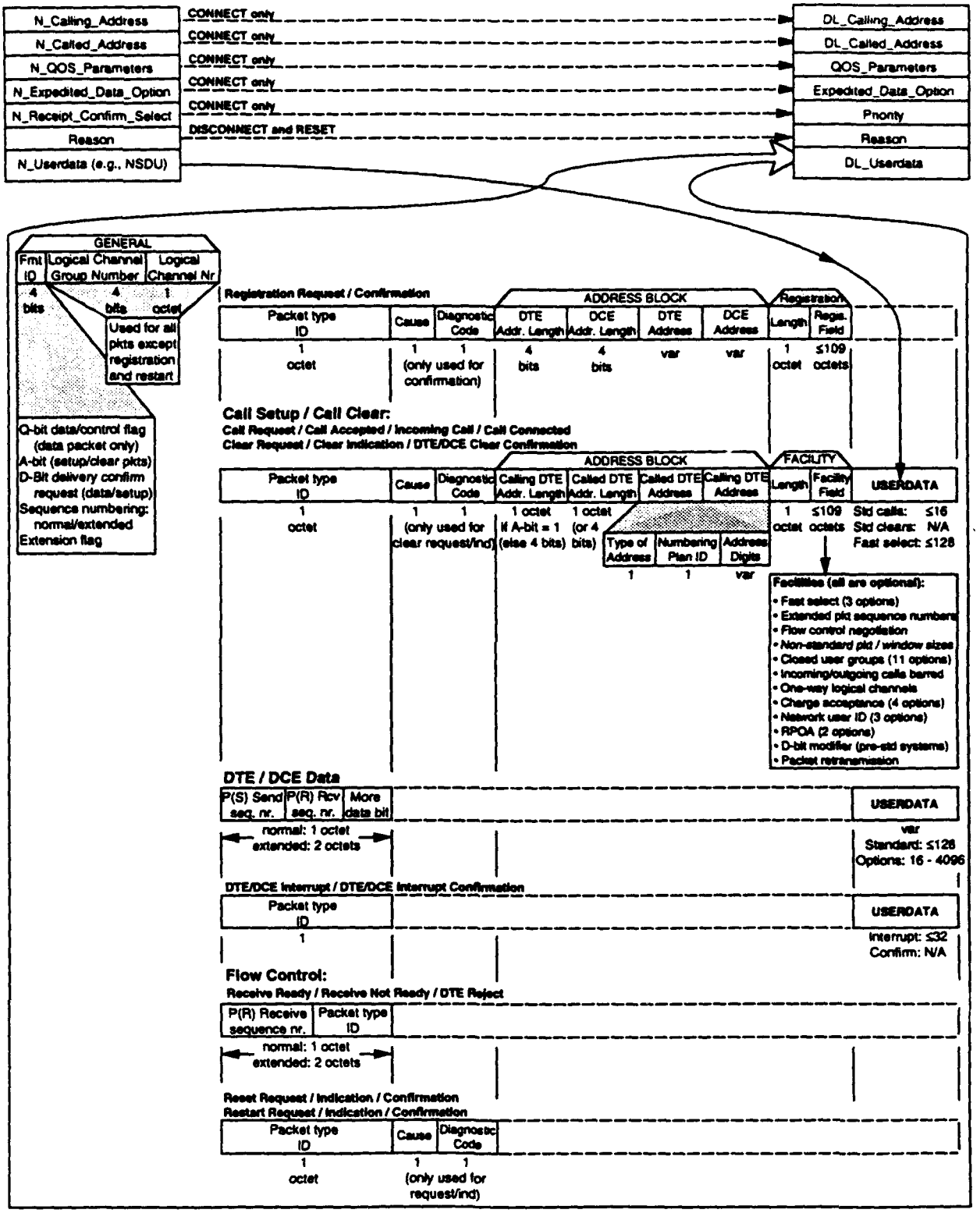


Figure 3.1-7. X.25 Packet Level Protocol Protocol Data Units

receiver can accept. Reset is used to reinitialize the packet send and receive numbers to zero for both the DTE and DCE on a single logical channel. The Restart procedure is used for more extensive recovery. It reinitializes the entire Packet Layer DTE/DCE interface by resetting all switched and permanent virtual circuits on the link to zero.

3.1.8 Link Access Procedures - B (LAPB)

The Link Access Procedures - B (LAPB) [CCITT 88] are described in the X.25 Recommendation as the Data Link Layer Element used for data interchange between a DCE and a DTE over a single physical circuit (single link procedures, or SLP) or over multiple circuits (multilink procedures, or MLP). LAPB is the protocol that is used to provide Data Link Layer services to X.25. LAPB and X.25 are part of a stack that provides lower layer connection-oriented communications for WAN connectivity.

The LAPB PDUs, shown in **Figure 3.1-8**, are similar to connection-oriented Type 2 LLC which provides acknowledgment (via ACK PDU), flow control (via sequence numbering and Receive Ready / Receive Not Ready), and error recovery (via Reject). LAPB has *Information, Flow Control, SABME/Disconnect, and Frame Reject* PDUs.

All of the LAPB PDUs begin with a one-octet Start Flag and one-octet Destination Address. All of the PDUs end with a two-octet Frame Check Sequence and a one-octet End Flag. The only differences between the various types of PDUs are how the control fields are encoded and whether an information field is present. The control fields in the Information and Flow Control PDUs contain sequence numbers, but the connection establishment PDU does not. Sequence numbers are included in the Frame Reject PDU as information. Only the Information PDU contains an SDU, although the Frame Reject Response PDU has an information field to provide a reason for rejecting the PDU and to provide current send and receive state variable values (i.e., sequence numbers).

Since a LAPB channel connects only one DCE to one DTE, the destination address does not identify the DCE or DTE, but identifies whether the frame is a command or a response and whether it is a single link or multilink operation.

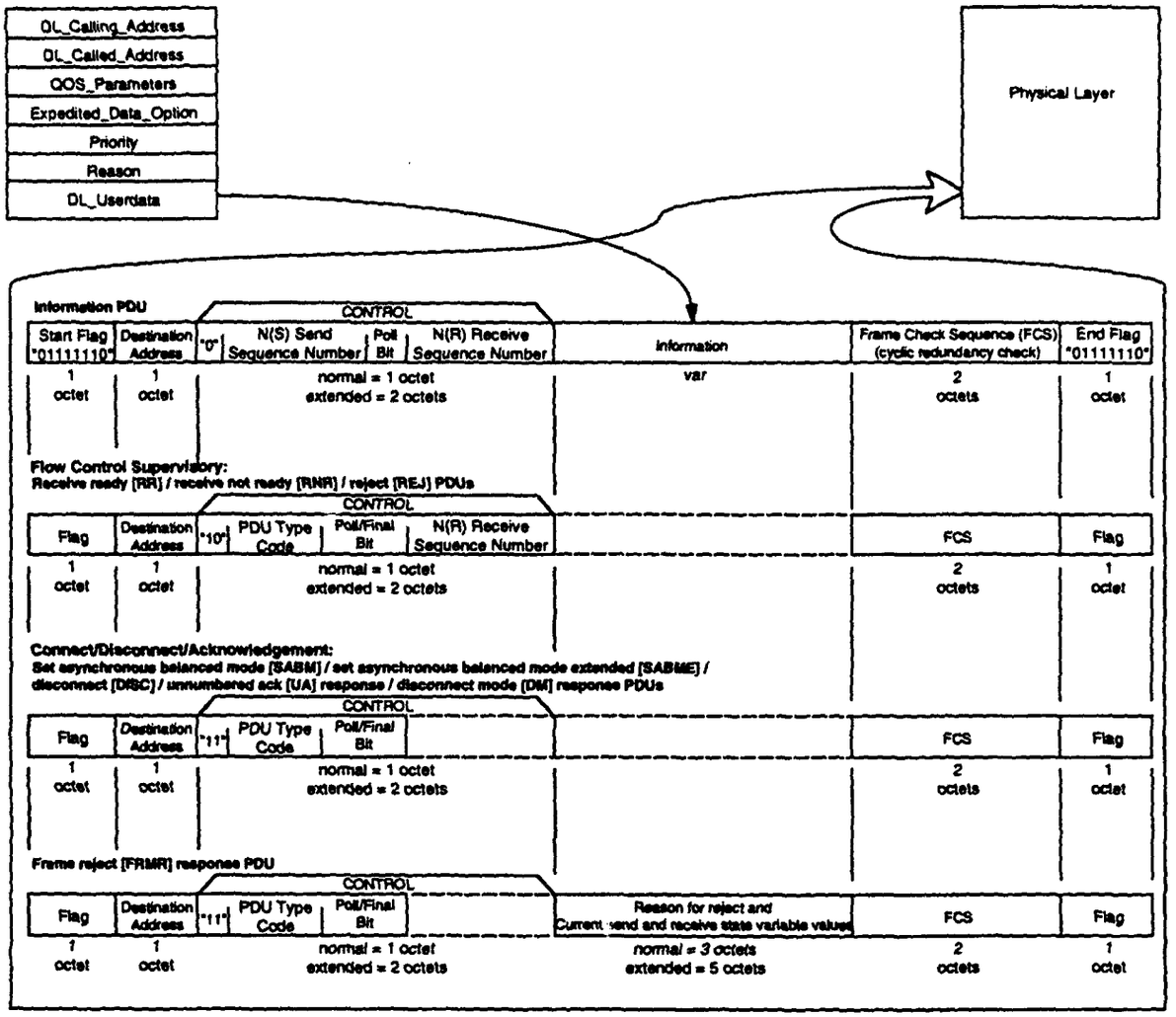


Figure 3.1-8. Link Access Procedures - B (LAPB) Protocol Data Units

3.2 LAN Protocol Descriptions

The Data Link Layer is split into two sublayers by the IEEE 802 standards: the logical link control (LLC) sublayer at the top of Layer 2, and the media access control (MAC) sublayer at the bottom. Both sublayers add headers to PDUs, and the MAC sublayer adds a trailer. All of the LAN-oriented protocols discussed in this report are *bit-oriented*; they use a specific bit pattern to delimit start and end points for synchronization purposes and prohibit the use of the pattern at any other spot within a frame. The following LAN-oriented generic communications and security protocols are described in this section:

- ISO 8802-2 Logical Link Control (LLC)
- IEEE 802.10 Secure Data Exchange (SDE)
- ISO 9314 Fiber Distributed Data Interface (FDDI)
- ISO 8802-3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

3.2.1 Description of Logical Link Control Protocol (LLC)

The ISO 8802-2 Logical Link Control (LLC) [ISO 90B] is a peer-to-peer protocol that transfers information and control between any pair of Data Link Layer service access points on a LAN. There are two types of LLC: Type 1 which provides a connectionless mode with no acknowledgment, flow control, or error recovery, and Type 2 which provides connection oriented service with acknowledgment (via ACK PDU), flow control (via sequence numbering and Receive Ready / Receive Not Ready), and error recovery (via Reject PDU). Although Type 1 LLC has no acknowledgment, acknowledgments by higher layers can be used. In addition, IEEE is currently considering adding Type 3, an acknowledged connectionless service, to LLC. Type 3 acknowledgments will occur with a half-duplex protocol in which the source must wait for acknowledgment of the PDU before sending the next PDU.

As shown in **Figure 3.2-1**, there are two distinct classes of LLC operation: Class I provides only Type I connectionless service while Class II provides both Type 1 connectionless and Type 2 connection-oriented service. There are three basic Type 1 PDUs: *Unnumbered Information, Exchange ID, and Test PDUs.* There are four basic Type 2 PDUs: *Numbered Information, Set Asynchronous Balanced Mode Extended (e.g., Connect)/Acknowledgment/Disconnect, Frame Reject, and Flow Control.* (Note: fields that are less than one octet are separated in the diagram by lines which are shorter than those that separate full octet fields.)

Each Type 1 and Type 2 PDU carries the Source and Destination Service Access Point addresses, a flag indicating whether the addresses are individual or group (multicast) addresses, a flag indicating whether the PDU is a command or a response, control fields that identify the PDU type and, in the case of Type 2 Information and Flow Control PDUs, sequence numbers.

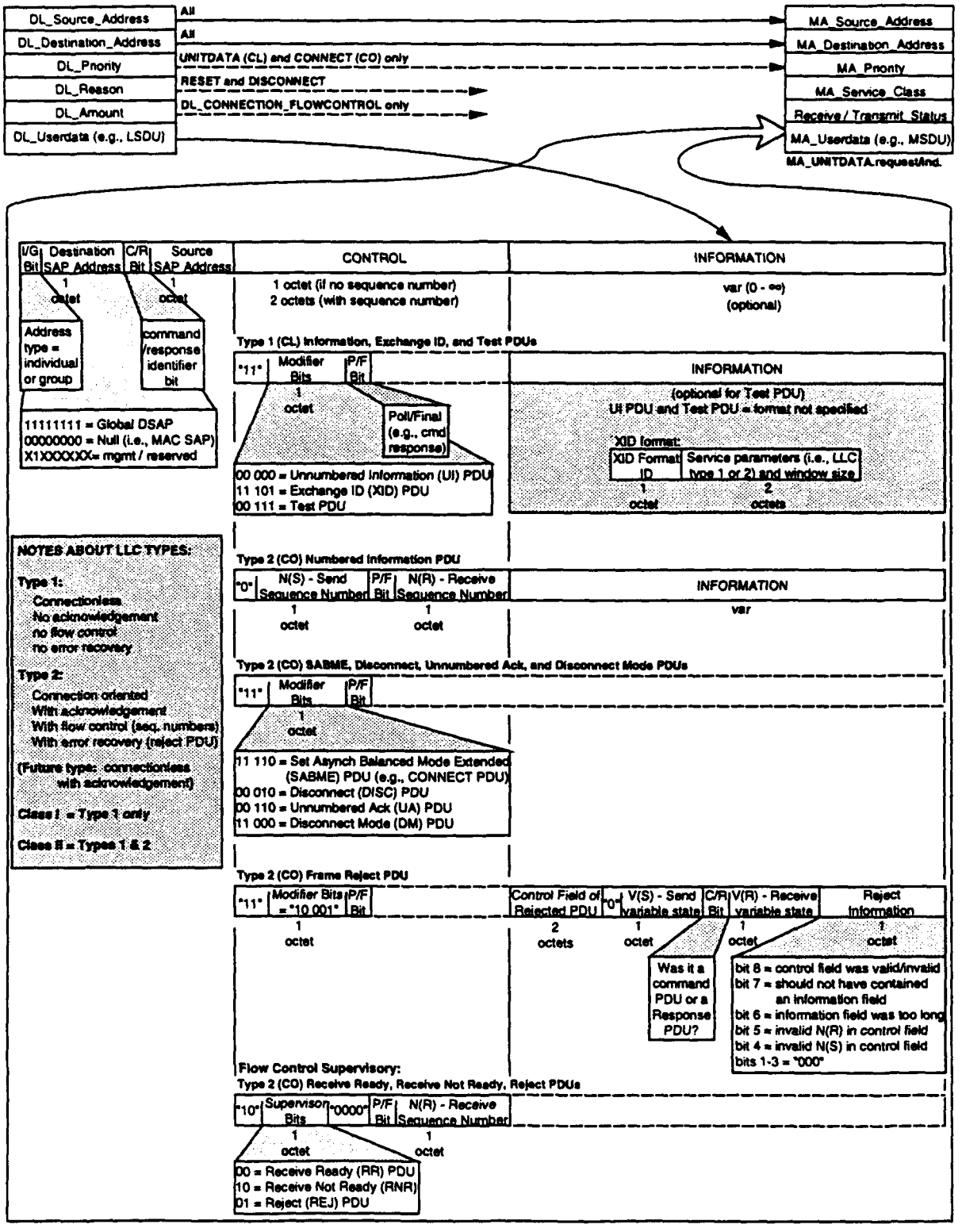


Figure 3.2-1. Logical Link Control (LLC) Protocol Data Units

3.2.2 Description of Secure Data Exchange Protocol (SDE)

The IEEE 802.10 Standard for Interoperable LAN/MAN Security (SILS) Clause 2 specifies the Secure Data Exchange (SDE) protocol. [93A] SDE is a security protocol that is designed to provide integrity and confidentiality services through encapsulation of LLC PDUs in a security envelope using encryption, an integrity check value (ICV), or both. The data confidentiality and data integrity services can be provided end-to-end, ES-to-IS, or IS-to-IS. SDE also supports data origin authentication and access control through the use of key management provided by an external protocol operating at the Application Layer.

Security Labeling is being added to SDE. The label will be an option in the Protected Header that can be used to control access, specify protective measures, and identify handling restrictions required by the local security policy. Specification of the label is implementation specific, and can identify a DoD classification or range of classifications and additional compartments, protection categories, caveats, and handling restrictions. It could also identify other local labels such as company private, company confidential, proprietary, or any foreign specified markings.

Within an unbridged LAN, SDE will protect the data but will not hide the source and destination addresses since LANs operate in a broadcast mode where all stations have the potential to monitor traffic on the bus, or are ring topologies where traffic is repeated from station to station until it reaches the destination. For LANs connected by remote bridges, SDE security associations could be established to hide the source or destination address, or both, if one or both of the SDE protocol entities is located at a bridge.

As part of the LLC sublayer, the SDE entity provides a connectionless service immediately above the MAC sublayer. SDE augments standard LLC and MAC communications protocols without replacing those protocols. It provides transparent security across the MAC sublayer at the boundary to the LLC entity. [IEEE 93A] All of the parameters of the service request except the MAC Service Data Units (MSDUs) are copied unaltered from the SDE_UNITDATA.request to the MA_UNITDATA.request. SDE does not preclude the use of unprotected communications between LLC protocol entities and can therefore operate in LANs and MANs where not all stations use SDE.

The SDE PDU consists of an optional Clear Header that is not protected by encryption or an ICV, a Protected Header that can be protected by either or both, and Protected Data. The Clear Header contains LSAP address information, a group/individual indicator flag, a Security Association Identifier (SAID) field, and an optional management defined field (MDF). The MDF can be up to 20 octets and can be used for key exchanges or other local uses.

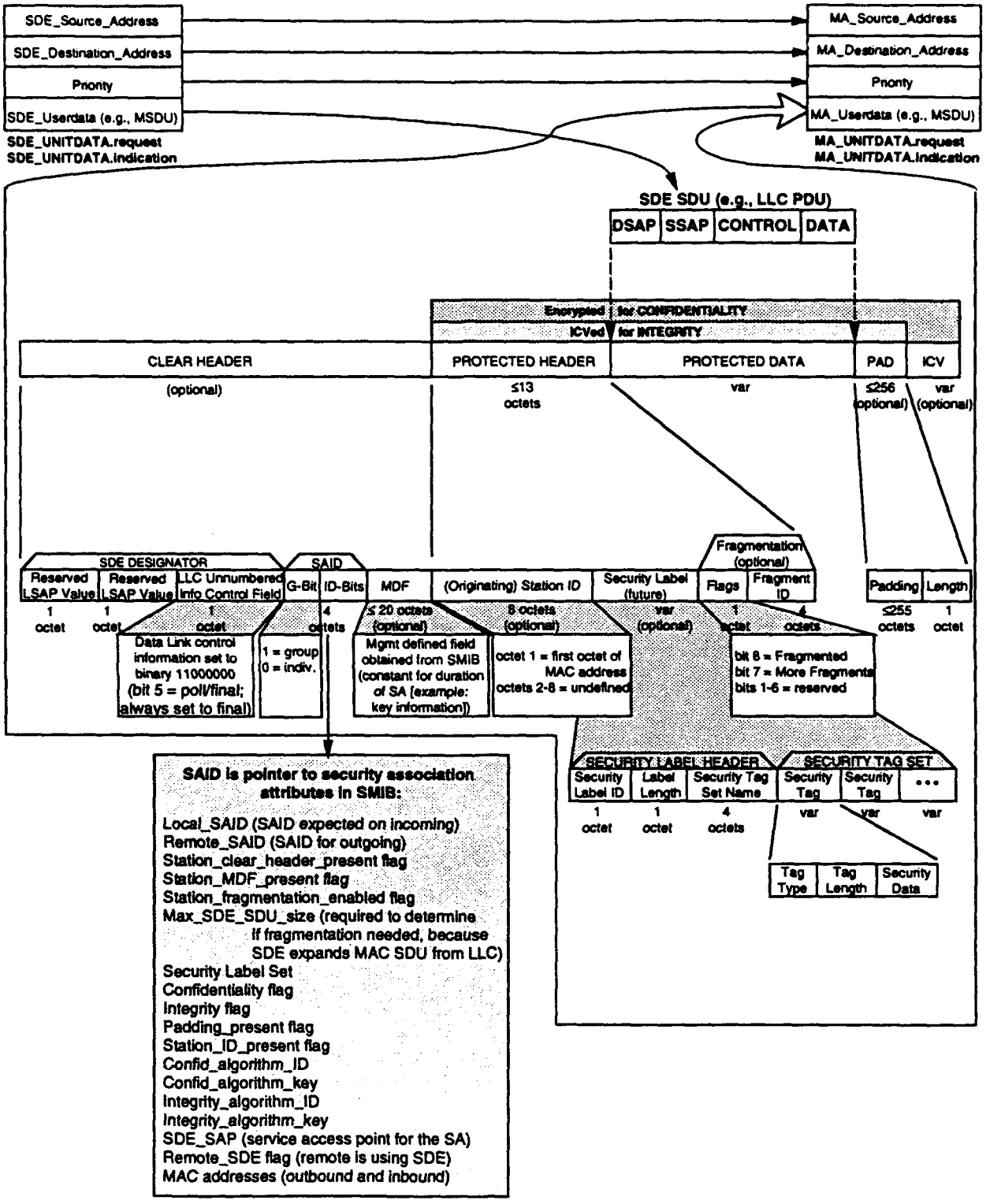


Figure 3.2-2. Secure Data Exchange (SDE) Protocol Data Unit

When the hosts negotiate a security association (SA) such that SDE PDUs transmitted between the two hosts will not have Clear Headers, then the receiving station will determine the SA and the correct protocol stack based on source and destination address parameters in the MA_UNITDATA.indication (i.e., the addresses passed down by LLC). SA attributes are maintained by both SDE peer-entities in their respective SMIBs. These attributes are accessible by system management, security management, and key management protocols. Multiple SAs can exist at any time, each being established during a system or key management exchange, but only one can apply to an SDE PDU.

The Protected Header consists of the Originating Station ID, a security label, an optional Fragmentation Block since SDE performs fragmentation of MSDUs to meet the size limitations of the MAC protocol, and Protected Data. Padding can optionally be added to meet the needs of the integrity and confidentiality algorithms.

3.2.3 Description of Fiber Distributed Data Interface (FDDI)

The Fiber Distributed Data Interface (ISO 9314) [ISO 89B, 89C, and 90A] consists of a Physical Layer, which provides the fiber optic medium and connectors, a MAC Data Link sublayer which provides access to the medium, address recognition, and frame generation, an LLC Data Link sublayer which provides a common protocol for data assurance services between MAC and the Network Layer, and Station Management which provides station level control on the ring. The FDDI MAC sublayer protocol (ISO 9314-2) processes data using 5-bit symbols. While each symbol has five bits, only four are information bits so that there are never more than two zeros or two ones in a row. This is necessary in order to derive a clock signal for synchronization. Therefore, the FDDI transmission rate is 125 Mbps while the effective information rate is only 100 Mbps.

The PDU, shown in **Figure 3.2-3**, can be up to 9,000 symbols in length (4,500 octets of information, or 5,633 bytes for transmission). There are 16 data symbols (hex 0 through F) and six control symbols represented by the letters I, J, K, R, S, and T. The symbol "I" is used to indicate the normal condition of Idle on the medium between transmissions. The Idle symbol provides a continuous fill pattern to establish and maintain clock synchronization. Symbols J and K are combined for the starting delimiter. T is used as the ending delimiter. A sequence of three or more R and S symbols (Reset and Set, respectively) are used to indicate the frame status.

An FDDI frame consists of a preamble that is at least 16 symbols of Idle, the "JK" starting delimiter, Frame Control information, destination and source addresses, an individual/group address flag, data (e.g., MAC SDU), a Frame Check Sequence, the "T" ending delimiter, and the "RSRS" frame status. Repeater stations may shorten or lengthen the preamble as necessary for Physical Layer clocking requirements.

Service class (asynchronous or synchronous) and other Frame Control information are taken from parameters of the MA_UNITDATA. Source and Destination addresses may be either 16 or 48 bits in length (4 or 12 symbols) which is equivalent to

the 2 or 6 octets used by ISO 8802-3 CSMA/CD in normal and extended addressing modes, respectively. All stations are required to be 16-bit address capable and be capable of functioning in a ring with stations concurrently operating with 48-bit addresses. The frame check sequence (FCS) field is eight symbols, or 32 information bits, which is equivalent to the 4 octets allocated in CSMA/CD.

Being a token ring topology, FDDI passes the right to transmit from one station to another via a Token PDU. An FDDI Token PDU consists only of the preamble, the "JK" starting delimiter, Frame Control information, and the "T" ending delimiter.

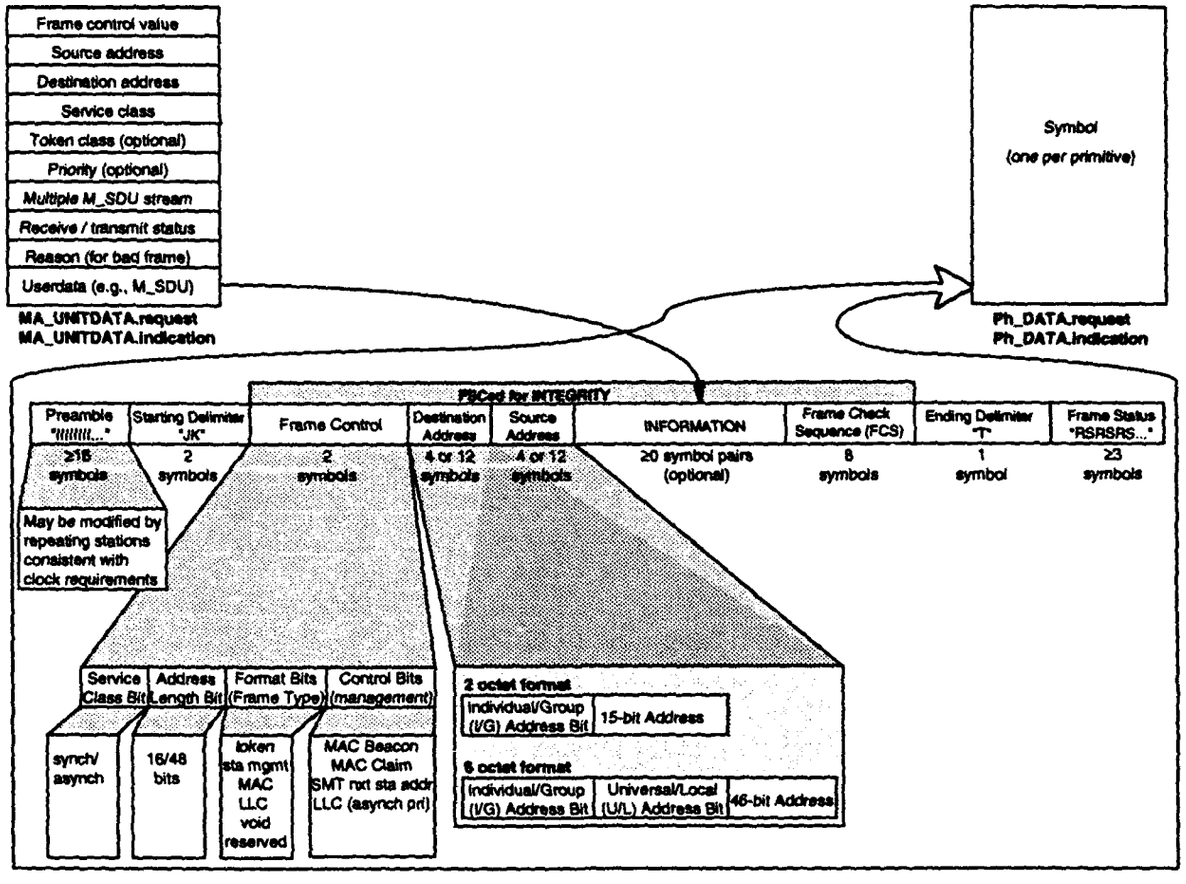


Figure 3.2-3. Fiber Distributed Data Interface (FDDI) Protocol Data Unit

3.2.4 Description of 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

The ISO 8802-3 (commonly referred to as IEEE 802.3) Carrier Sense Multiple Access with Collision Detection (CSMA/CD) [ISO 93] protocol data unit, shown in **Figure 3.2-4**, is a MAC sublayer protocol similar to FDDI. The CSMA/CD PDU begins with a preamble consisting of alternating ones and zeros for clock synchronization, and a one-octet start frame delimiter. Source and destination addresses may be 16 or 48 bits in length. Padding needed for proper collision detection and timing requirements are added in a pad field to make the frame a minimum of 64 octets from the destination address to the FCS, inclusive. The PDU is completed with a Frame Check Sequence field.

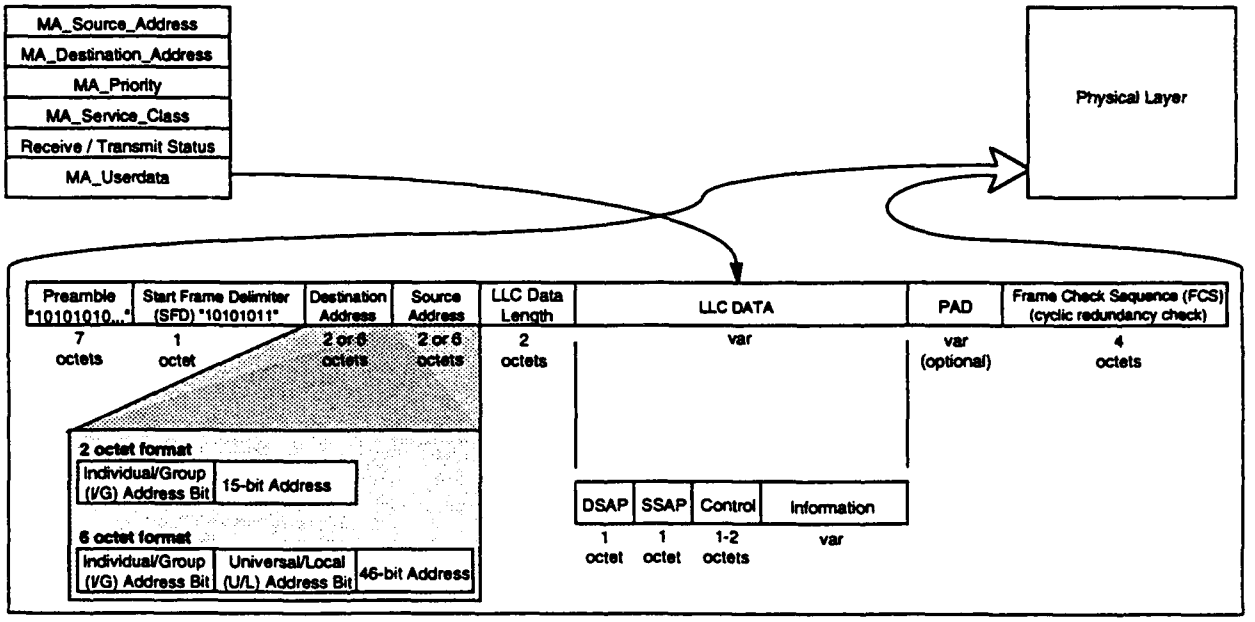


Figure 3.2-4. ISO 8802-3 CSMA/CD Protocol Data Unit

3.3 Summary of Protocol Characteristics

The WAN-oriented protocols considered during this analysis operate at the Transport, Network, and Data Link Layers. They include the Connection Oriented Transport Protocol, Classes 1 and 4 (TP1 and TP4), the Connectionless Network Protocol (CLNP), the X.25 Packet Level Protocol, Link Access Procedures - B (LAPB), and four security protocols (TLSP, SP4, NLSP, and SP3).

TP1, TP4, and X.25 are connection-oriented and have control PDUs to establish and clear connections, reject PDUs, acknowledge receipt of DATA PDUs, and so forth. Once an end-to-end connection is established, they exchange DATA PDUs which only have fields for connection ID, data, and sequence numbers. CLNP is connectionless and incorporates both data and all control information (e.g., addresses, segmentation, padding, source routing, and QOS parameters) into one PDU, the UNITDATA PDU.

LAPB (operating under X.25) is connection-oriented and has Control PDUs to establish and clear connections, reject frames, and provide flow control. Once the connection is established, it exchanges Information PDUs. The primary fields of LAPB Control and Information PDUs are start and end flags, the Poll/Final Bit, sequence numbers, and the FCS. Information PDUs also have an information field.

The security protocols support both connectionless and connection-oriented communications protocols. They perform security encapsulation of protected control information (*security label, reflection* bit, padding, and Network Layer addresses (NLSP and SP3 except mode SP3N)) and Userdata of the SDUs that are passed to them from the layer or sublayer above. Encapsulation includes calculation of integrity check values over the Protected Headers and Userdata, and encryption of the same blocks and the ICV field. NLSP and TLSP are both capable of performing in-band key management or using keys established by out-of-band protocols. SP3 and SP4 must rely on external support for key establishment.

The LAN-oriented protocols considered during this analysis operate at the Data Link Layer. They include the Logical Link Control (LLC), Fiber Distributed Data Interface (FDDI), Carrier Sense Multiple Access with Collision Detection (CSMA/CD), and one security protocol (SDE).

Type 2 LLC is connection-oriented and has Control PDUs to establish and clear connections, reject frames, and provide flow control. Once the connection is established, it exchanges Information PDUs. The primary fields of Type 2 LLC Control and Information PDUs are the LSAPs, the Poll/Final Bit, and sequence numbers. Information PDUs also have an information field.

Type 1 LLC is connectionless with no acknowledgment, flow control, or error recovery and Type 2 LLC provides connection-oriented service with all three. FDDI and CSMA/CD are connectionless and incorporate all control information (including MAC addresses) into the DATA PDU. Other fields include start and end delimiters, frame check sequences, and of course information.

Secure Data Exchange provides connectionless LAN security with security encapsulation of LLC PDUs and a portion of its own header. SDE encapsulation includes calculation of integrity check values and encryption, just as does encapsulation performed by the security protocols that operate at the Network and Transport Layers.

This Page Intentionally Left Blank

Section 4

Analysis of Protocol Control Information

This Page Intentionally Left Blank

4.0 Analysis of Protocol Control Information

There are two basic architectural options for providing end-to-end encryption services at a given layer:

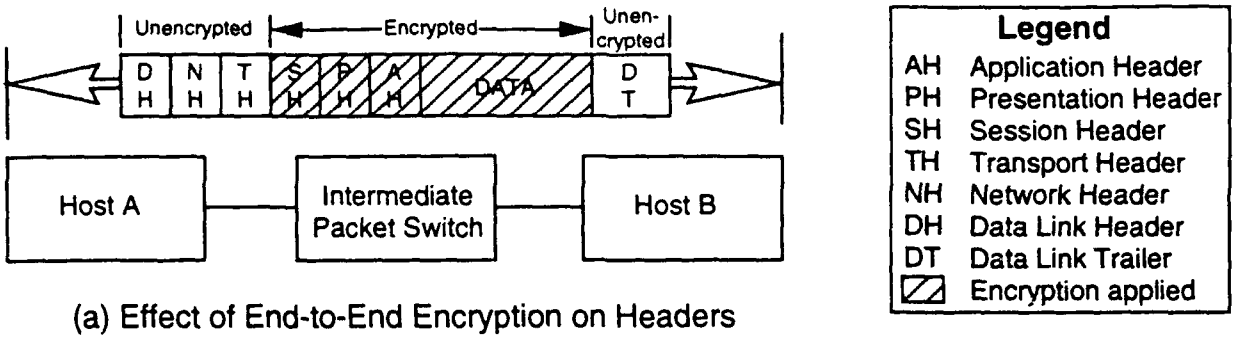
- Encrypt the Service Data Unit (SDU) provided from the layer above, and send the header generated within the layer in the clear
- Encrypt both the SDU provided from the layer above, and the header (or portions of the header) generated within the layer itself.

All of the headers below the layer at which the encryption mechanism operates are sent in the clear, as is usually the header generated within the layer itself. This characteristic of end-to-end encryption when provided in computer networks with no link encryption being provided in a lower layer is illustrated in **Figure 4.0-1(a)**. The effect of using link level encryption alone in a computer network is illustrated in **Figure 4.0-1(b)**. Lower layer headers (as well as higher layer headers) can be encrypted over the physical link when link encryption is used. The disadvantage is that the headers and data are not encrypted at Intermediate Systems (e.g., packet switches and gateways) when link encryption is used alone. Thus, in these cases, the intermediate packet switch must be sufficiently trustworthy, be contained in a sufficiently trustworthy facility, and be operated in a sufficiently trustworthy manner.

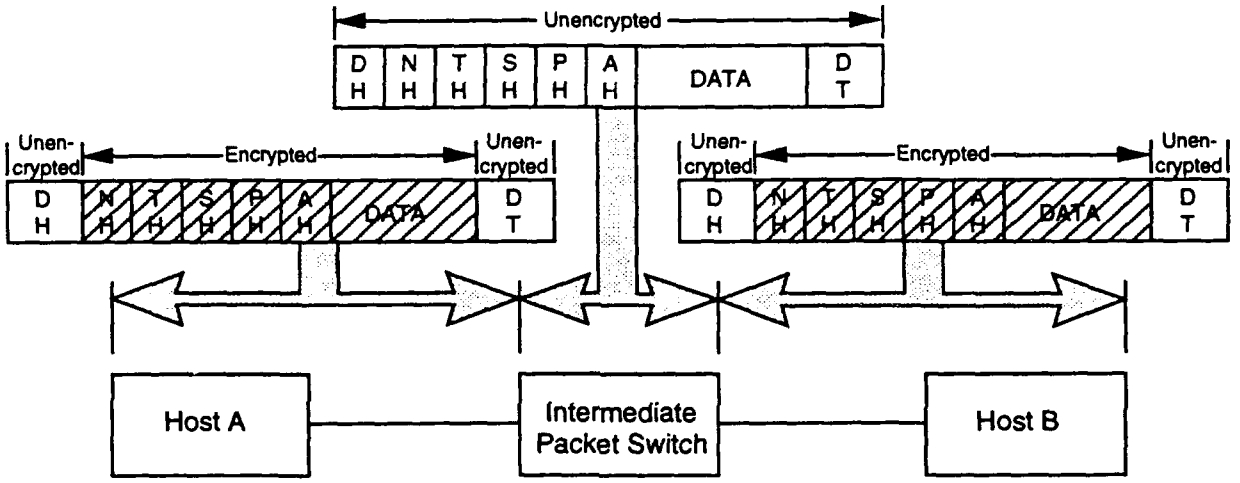
Another problem with sending lower layer protocol control information in the clear is that the user information being sent over the physical link is framed by the PCI. A special flag is used to identify the beginning and end of the frame. This same pattern is also used in several data link protocols to indicate that the channel is idle. This characteristics serves to convey the size of the PDUs being sent over the physical link. An adversary can measure the amount of traffic being sent over physical links by monitoring the idle/delimiter flag characters. An adversary can infer mission-oriented information by establishing the flow and amount of traffic that is sent through a network. The process of analyzing a network from this perspective is referred to as *traffic analysis*. Techniques which protect against traffic analysis are said to provide *traffic flow confidentiality*.

There are advantages to employing a combination of both end-to-end and link encryption mechanisms in a computer network. This is the case when end-to-end encryption features are required, but the risk of passing headers in the clear is too great to ignore the need for link encryption within one of the lower layers (Network, Data Link, or Physical) as well. To perform both end-to-end encryption and link encryption requires that upper and lower layer security protocols be implemented at both End Systems (or the gateways to the secure subnetworks where the End Systems are located) and that a lower layer security protocol be implemented at Intermediate Systems.

The nature of the protocol control information available at lower layers provides a basis for determining the advantages and disadvantages of providing link encryption at the different lower layers. It is necessary to determine the extent of the vulnerabilities associated with sending lower layer OSI headers in the clear in order to eliminate or reduce the traffic flow confidentiality problem.



(a) Effect of End-to-End Encryption on Headers



(b) Effect of Link Encryption on Headers

Figure 4.0-1. Effect of Encryption on Headers

The objective of this section is to analyze the information that is available in the headers and trailers of the PDUs (information and control), and assume the role of a traffic analyst attempting to determine what types of mission-related information can be inferred. To accomplish this, inferences are drawn based on the information available in the headers and trailers. *(Note: trailers generally include only the error detection code and, in the case of Data Link Frames, ending delimiters. Therefore, the discussion and figures generally refer to the headers.)* Although the protocol entities within a given layer only generate and process their associated layer headers, a traffic analyst viewing header information transmitted over a physical link can analyze all of the headers that are sent in the clear and make inferences based on this collective information.

The degree of vulnerability associated with the inferences that can be drawn by the enemy forms the basis for establishing the severity of the traffic flow confidentiality problem and the types of traffic flow confidentiality mechanisms needed to provide protection services.

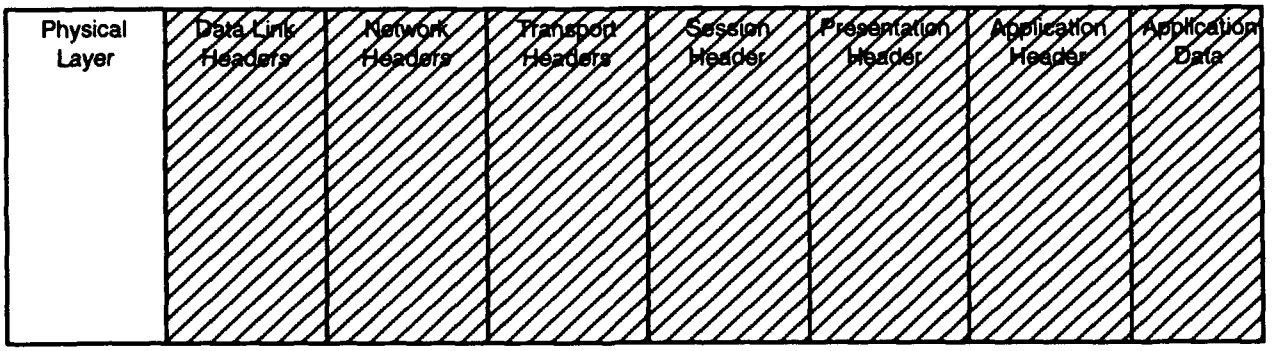
There are two primary attack methods that an adversary might use to intercept and modify message traffic. First, the intruder can wiretap into a channel between two points. In this case, the intruder is likely to monitcr traffic, and could replay valid traffic and insert spurious traffic. These latter events could disrupt control of communications. (If the data is encrypted, the spurious data would not be decrypted and passed as valid data.) Second, the adversary may take control of a valid station and use it to intercept traffic. This might occur through subversion of an authorized user, or the adversary may simply be a disgruntled user. If the adversary controls a station on a LAN employing a ring topology or an Intermediate System on a WAN, that adversary is in an ideal position to modify traffic because that station is expected to receive and retransmit every PDU in order for the network to function properly.

Section 4.1 briefly discusses security features that are inherent in the protocols and which are effective in preventing disclosure, delay, corruption, and loss of PDUs.

Section 4.2 discusses the security relevant fields in the headers of a typical LAN stack and evaluates what is exposed to interception when no security protocols are applied and when security protocols are applied in Layers 4, 3, and 2.

Section 4.3 discusses the security relevant fields in the headers of a typical WAN stack and evaluates what is exposed to interception when no security protocols are applied and when security protocols are applied in Layers 4, and 3. Secure Data Exchange, the Data Link Layer security protocol, is designed to only operate with LANs and Metropolitan Area Networks (MANs).

Another option is to implement full period encryption at the Physical Layer in order to hide all protocol control information of the higher layers. The effect of full period encryption is shown in **Figure 4.0-2**. This approach is effective against the first method of attack because a wiretapper cannot directly observe any data or header information. This approach is not effective against the second method of attack where an adversary takes control of an authorized station since full period encryption is applied individually across each link and the message traffic is decrypted at each intermediate station.



Shading indicates that encryption is applied and no information is in the clear.

Figure 4.0-2. Full Period Encryption at Layer 1

4.1 Inherent Security Features of the Protocols

Each of the protocols have features that help provide security against disclosure, delay, corruption, and loss of PDUs. While the traffic analyst is interested in identifying weaknesses (discussed in **sections 4.2** and **4.3**), the security features, whether intended for security or for efficiency, are of interest. It should be noted that these features may rely on information that is placed unprotected in the header. For example, transport sequence numbers enhance security for the information but are themselves not secure. They rely on other mechanisms for their security. In such cases, it is important to protect the PDU by encrypting it at a lower layer.

Figure 4.1-1(a) identifies security features of the LAN-oriented protocol stack. Figures (b), (c), (d), (e), and (f) show the stack with TLSP, SP4, NLSP, SP3, and SDE, respectively.

Figure 4.1-2(a) identifies security features of the WAN-oriented protocol stack. Figures (b), (c), (d), and (e) show the stack with TLSP, SP4, NLSP, and SP3, respectively.

Important features that enhance security include:

- **Sequence numbering** – this connection-oriented capability provides connection integrity by preventing duplication, replay, insertion, and deletion. It also enables recovery. It is supported by TP4, Type 2 LLC, TP1, X.25, and LAPB. It is also supported by TLSP, SP4, NLSP, and SP3. Most protocols perform resequencing to correct misordering by the underlying service provider.

- **Final sequence numbering** – this provides protection against connection truncation (i.e., the deletion of the final PDUs of a connection) during connection release. NLSP provides this capability at the Network Layer and SP4 provides it at the Transport Layer in conjunction with TP4.

- **Segmentation** – this is also called *fragmentation* and is normally provided to meet size requirements of the underlying service provider. However, segmentation has a positive side effect in that it also serves to limit the amount of data that is available to an eavesdropper, particularly when the PDUs are transmitted through the network over different routes. Protocols that perform segmentation are TP4, TP1, NLSP, CLNP, X.25, and SDE. TP4 is an example where the segments can be routed over different paths because it allows the use of multiple network connections. Segmentation also serves to hide the actual size of the PDU such that it limits the eavesdroppers ability to determine PDU type and content when encryption is used.

802.3/FDDI Header	LLC Header	CLNP Header	TP4 Header	SH	PH	AH	
• checksum • zeros out unused fields (FDDI only)	• sequence no. (CO only) • flow control (CO only)	• segmentation • source routing • congestion indicator • lifetime • padding • checksum • security level (label) (option)	• sequence no. • segmentation • flow control • lifetime • checksum • protection param (label) (optional) • multiple N-connections				Application Data

(a) LAN Stack with no Security Protocol

802.3/FDDI Header	LLC Header	CLNP Header	TLSP Header	TP4 Header	SH	PH	AH	
• checksum • zeros out unused fields (FDDI only)	• sequence no. (CO only) • flow control (CO only) • security label (future)	• segmentation • source routing • congestion indicator • lifetime • padding • checksum • security level (label) (option)	• reflection bit • integrity sequence no. • padding • integrity check value • security label • zero out unused fields	• sequence no. • segmentation • flow control • lifetime • checksum • protection param (label) (optional) • multiple N-connections				Application Data

(b) LAN Stack with Transport Layer Security Protocol

802.3/FDDI Header	LLC Header	CLNP Header	SP4 Header	TP4 Header	SH	PH	AH	
• checksum • zeros out unused fields (FDDI only)	• sequence no. (CO only) • flow control (CO only)	• segmentation • source routing • congestion indicator • lifetime • padding • checksum • security level (label) (option)	• reflection bit • integrity sequence no. • final seq. no. • padding • integrity check value • security label	• sequence no. • segmentation • flow control • lifetime • checksum • protection param (label) (optional) • multiple N-connections				Application Data

(c) LAN Stack with Security Protocol 4

802.3/FDDI Header	LLC Header	CLNP Header	NLSP Header	TP4 Header	SH	PH	AH	
• checksum • zeros out unused fields (FDDI only)	• sequence no. (CO only) • flow control (CO only)	• segmentation • source routing • congestion indicator • lifetime • padding • checksum • security level (label) (option)	• reflection bit • integrity sequence no. • final seq. no. • segmentation • padding • ICV • security label	• sequence no. • segmentation • flow control • lifetime • checksum • protection param (label) (optional) • multiple N-connections				Application Data

(d) LAN Stack with Network Layer Security Protocol

802.3/FDDI Header	LLC Header	CLNP Header	SP3 Header	TP4 Header	SH	PH	AH	
• checksum • zeros out unused fields (FDDI only)	sequence no. (CO only) • flow control (CO only)	• segmentation • source routing • congestion indicator • lifetime • padding • checksum • security level (label) (option)	• reflection bit • padding • integrity check value • security label	• sequence no. • segmentation • flow control • lifetime • checksum • protection param (label) (optional) • multiple N-connections				Application Data

(e) LAN Stack with Security Protocol 3

802.3/FDDI Header	SDE Header	LLC Header	CLNP Header	TP4 Header	SH	PH	AH	
• checksum • zeros out unused fields (FDDI only)	• reflection bit • segmentation • integrity check value • padding • security label (future)	• sequence no. (CO only) • flow control (CO only)	• segmentation • source routing • congestion indicator • lifetime • padding • checksum • security level (label) (option)	• sequence no. • segmentation • flow control • lifetime • checksum • protection param (label) (optional) • multiple N-connections				Application Data

(f) LAN Stack with Secure Data Exchange Protocol

Figure 4.1-1. LAN Stack Security Features

LAPB Header	X.25 Header	CLNP Header	TP1 Header	SH	PH	AH	
• sequence no. • flow control • checksum (FCS) • can use multiple links	• sequence no. • segmentation • flow control	• segmentation • source routing • congestion indicator • lifetime • padding • checksum • security level (label) (option)	• sequence no. • segmentation • protection params (label) (optional)				Application Data

(a) WAN Stack with no Security Protocol

LAPB Header	X.25 Header	CLNP Header	TLSP Header	TP1 Header	SH	PH	AH	
• sequence no. • flow control • checksum (FCS) • can use multiple links	• sequence no. • segmentation • flow control	• segmentation • source routing • congestion indicator • lifetime • padding • checksum • security level (label) (option)	• reflection bit • integrity sequence no. • padding • integrity check value • security label • zero out unused fields	• sequence no. • segmentation • protection params (label) (optional)				Application Data

(b) WAN Stack with Transport Layer Security Protocol

LAPB Header	X.25 Header	CLNP Header	SP4 Header	TP1 Header	SH	PH	AH	
• sequence no. • flow control • checksum (FCS) • can use multiple links	• sequence no. • segmentation • flow control	• segmentation • source routing • congestion indicator • lifetime • padding • checksum • security level (label) (option)	• reflection bit • integrity sequence no. • padding • integrity check value • security label	• sequence no. • segmentation • protection params (label) (optional)				Application Data

(c) WAN Stack with Security Protocol 4

LAPB Header	X.25 Header	CLNP Header	NLSP Header	TP1 Header	SH	PH	AH	
• sequence no. • flow control • checksum (FCS) • can use multiple links	• sequence no. • segmentation • flow control	• segmentation • source routing • congestion indicator • lifetime • padding • checksum • security level (label) (option)	• reflection bit • integrity sequence no. • final seq. no. • segmentation • padding • ICV • security label	• sequence no. • segmentation • protection params (label) (optional)				Application Data

(d) WAN Stack with Network Layer Security Protocol

LAPB Header	X.25 Header	CLNP Header	SP3 Header	TP1 Header	SH	PH	AH	
• sequence no. • flow control • checksum (FCS) • can use multiple links	• sequence no. • segmentation • flow control	• segmentation • source routing • congestion indicator • lifetime • padding • checksum • security level (label) (option)	• reflection bit • padding • integrity check value • security label	• sequence no. • segmentation • protection params (label) (optional)				Application Data

(e) WAN Stack with Security Protocol 3

Figure 4.1-2. WAN Stack Security Features

- **Reflection bit** – this feature protects against playback by indicating whether the sender is the initiator or responder of the security association. It is typically implemented with a single-bit Direction Indicator Flag, commonly called the Initiator-Responder Flag. It is implemented in all five security protocols.

- **Source routing** – this can be used to ensure that traffic is routed over network components that are known to provide acceptable security services and to avoid network components that do not. Source routing is provided only by CLNP.

- **Connection flow control** – this is provided by connection-oriented protocols that use Receive Ready and Receive Not Ready PDUs in conjunction with sequence numbers so that the sending station will not transmit more information than the receiving station can accept and process. It helps protect against loss of PDUs. Protocols that provide connection flow control are TP4, X.25, LAPB, and Type 2 LLC.

- **Congestion notification** – CLNP is the only protocol to include this feature. It is implemented by a single bit that can be set by any Intermediate System (IS) to indicate that the PDU has encountered congestion. Subsequent ISs are not permitted to reset the bit. The information may be useful to the destination host in establishing source routes for future traffic.

- **Lifetime counter** – this is used to determine whether a PDU received may be forwarded by an IS or should be discarded in order to limit the possibility of network congestion. CLNP implements a counter that is decremented by each IS according to how long it expects to delay the PDU. Each number represents 500 millisecond of delay. TP4 also has an NSDU lifetime timer which represents the maximum time which may elapse between the transmission of an NSDU from the local transport entity to the network and receipt of any copy of the NSDU from the network at the remote transport entity.

- **Padding** – this is used to meet the block size requirements of encryption and integrity algorithms or the underlying transmission service, and to provide traffic flow confidentiality. CSMA/CD uses padding to meet channel sensing requirements and CLNP uses it for octal alignment. All of the security protocols implement padding to meet encryption and integrity algorithm requirements. In addition, NLSP uses padding to support traffic flow confidentiality.

- **Checksum** – this provides an integrity mechanism to detect corruption. All five security protocols support calculation and encapsulation of a secure integrity check value (ICV). Other protocols use non-secure error detection codes. CLNP provides a checksum feature. LAPB, FDDI, and CSMA/CD compute a cyclic redundancy check that is placed in the Frame Check Sequence field. When checksums are used in conjunction with encryption that includes error extension, an adversary cannot modify the PDU and then modify the check value to hide the fact that the PDU has been modified.

- **Security label** – this optional feature is used to support mandatory access control and routing decisions. A security label can be specified in TP4 and TP1 (in the protection parameter field), CLNP (in the security level field), and in all of the security protocols (in the label field). While a security label can be optional at any particular layer, the use of labels in at least one layer is mandatory for multilevel security.

- **Zeroing out unused or reserved fields and padding fields** – this prevents the field from being used as a covert storage channel. However, the value of preventing unused, reserved, and padding fields from being used is limited because there are more effective methods for two parties to communicate. For example, they can communicate directly by using the data field of a PDU. The protocols that zero out unused, reserved, and padding fields are TLSP and FDDI.

The security protocols provide similar services, as shown in **Figure 4.1-3**. All five protocols are transparent. In other words, the protocols do not preclude the use of unprotected communications and can therefore operate in networks where not all stations use those protocols.

NLSP and TLSP provide full in-band key management, and SDE operates with a companion protocol to also provide key management. SP3 and SP4 must rely on external protocols for key management. SDE, NLSP, and TLSP work with either asymmetric or symmetric encipherment. SP3 does not specify the method and SP4 assumes the use of symmetric encipherment.

SDE and SP3 provide connectionless security services while NLSP, SP4, and TLSP provide both connection-oriented and connectionless services. All five protocols can carry security labels and can support access control based on those labels. All five protocols have features to protect against reflection. SDE and NLSP perform segmentation in order to meet size requirements of the underlying transmission service. Only TLSP zeros out unused, reserved, and padding fields.

	SDE	SP3	NLSP	SP4	TLSP
Transparency on network	Yes	Yes	Yes	Yes	Yes
Address/QOS parameter hiding	Yes	Yes (4)	Yes	Yes	Yes
In-band key management	Yes (1)(2)	No	Yes (6)	No	Yes (9)
Diffie-Hellman key exchange	Yes (1)	No	Yes	No	Yes
Accepts either symmetric or asymmetric	Yes (1)	UNK (5)	Yes	No (7)	Yes
CONNECTION ORIENTED:					
– PE Authentication (through third party)	n/a	UNK (5)	Yes	Yes	Yes (10)
– Confidentiality	n/a	UNK (5)	Yes	Yes	Yes
– Integrity (with/without recovery)	n/a	UNK (5)	No/Yes	Yes	Yes
– Integrity sequence numbering *(Insertion, deletion, replay protection)*	n/a	No	Yes	Yes	Yes
– Final sequence number checking *(Connection truncation protection)*	n/a	No	Yes	Yes	No
– Retain-on-disconnect	n/a	No	Yes	No	Yes
– Require separate key per connection *(Connection replay protection)*	n/a	No	Yes	Yes (8)	No
CONNECTIONLESS:					
– DO Authentication (by ICV and KM)	Yes	Yes	Yes	Yes	Yes
– Confidentiality	Yes	Yes	Yes	Yes	Yes
– Integrity	Yes	Yes	Yes	Yes	Yes
– Traffic flow confidentiality (padding)	No (11)	No (11)	Yes	No (11)	No (11)
– Source routing	n/a	Yes (12)	Yes (12)	No	No
– Route recording	n/a	Yes (12)	Yes (12)	No	No
Access control level (label, keys, authenticated addresses)	Yes	Yes	Yes	Yes	Yes
Label set	Yes	Yes	Yes	Yes	Yes
Direction indicator [Initiator-Responder flag] *(reflection protection)*	Yes (3)	Yes	Yes	Yes	Yes
Fragments/segments to meet size rqmts	Yes	No	Yes	No	No
Zeros out unused/reserved fields	No	No	No	No	Yes

Note 1: IEEE 802.10 includes the Key Management Protocol which provides in-band key management for SDE, including the optional uses of a Diffie-Hellman key exchange and connection key management based on X9.17.
Note 2: Keys could be passed in the SDE management defined field (MDF) if implemented locally.
Note 3: LAN addresses are sufficient indication of direction in the Data Link layer. Therefore, the Poll/Final bit taken from the LLC PDU is always set to Final.
Note 4: SP3 addressing modes SP3A, SP3D, and SP3I provide address/QOS hiding; SP3N does not.
Note 5: The encryption method and the connection-oriented security services may be defined external to SP3 but used in conjunction with SP3.
Note 6: NLSP Connection Security Control (CSC) PDU provides in-band keying.
Note 7: SP4 allows only symmetric keying.
Note 8: SP4C (CO) requires separate keys per connection; not applicable to SP4E (CL).
Note 9: TLSP uses the Security Association (SA) PDU to provide in-band keying.
Note 10: TLSP peer-entity authentication includes certification by a trusted third party Certification Authority.
Note 11: SDE, SP3, SP4, and TLSP have padding fields. However, those fields are intended to accommodate encipherment and integrity algorithm block size requirments, rather than traffic flow confidentiality.
Note 12: CLNP performs routing services, but NLSP and SP3 can support their performance.

Figure 4.1-3. Comparison of Services and Features in Lower Layer Security Protocols

4.2 Security Relevant Information in a LAN-Oriented Stack

The OSI stack being considered in this section includes the most common LAN protocol, ISO 8802-3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD), and the emerging LAN protocol for fiber optic media, ISO 9314 Fiber Distributed Data Interface (FDDI). It also includes the protocol for the Logical Link Control (LLC) sublayer in the ISO 8802-2 Local Area Network Protocol. LANs are often interconnected, so the stack also includes the ISO 8473-1 Connectionless Network Protocol (CLNP) and the ISO 8073 Connection Oriented Transport Protocol, Class 4 (TP4). The full stack is illustrated in **Figure 4.2-1**.

802.3/FDDI Header	LLC Header	CLNP Header	TP4 Header	SH	PH	AH	
• source address • dest address within the LAN • length (of LLC PDU) (FDDI: derived from delimiters) • checksum (FCS)	• link SSAP • link DSAP	• network SSAP • network DSAP • source routing • route record • congestion notification • priority • lifetime • security level • segment length • checksum	• transport SSAP • transport DSAP • connection ref. • priority • ack time • security label • segment length • sequence no. • flow control • checksum				Application Data

Figure 4.2-1. LAN Security Relevant Parameters Exposed to Interception

Information about the traffic being passed between two hosts can be derived from the transport header because the Transport Layer provides end-to-end connectivity. The TP4 Connection Request PDU identifies the calling and called transport service access points (SSAP and DSAP) and establishes transport source and destination connection references that are visible in all other TPDUs.

The different SAPs at a given layer boundary provide access to different types of services. Examples include connection-oriented, connectionless, and security services. Different types of application processes and protocols often require access to different types of services (and therefore different SAPs) at the Transport Layer. For example, the use of a connectionless SAP at the Transport Layer often indicates that a query-response application is being supported. To map Transport Layer SAPs to the application processes and protocols being supported requires that collateral information about the system be acquired. This can often be accomplished by reviewing documentation on the particular system under observation.

TP4 Connection Request (CR) PDUs include a priority parameter which can be used by an adversary to gain some insight into the importance of the traffic to be sent over the connection. Collateral information on the specific system can be gathered to

determine how the priority parameter corresponds to the operational priorities of mission traffic. The CR PDU also includes acknowledge time and transit delay parameters which can be used by an adversary to better determine opportunities for attack and the effect of various strategies. A connection security label can be inserted into the TP4 protection parameter in a CR PDU. There is a potential for an adversary to modify this field which could result in incorrect routing decisions in cases where routing control is imposed to assist in providing security services.

TP4 performs segmentation which could hide the length of the TPDU if individual segments are routed differently over the network. Masking the length of the message helps to mask the type of message being transmitted. Sequence numbers are associated with each Data TPDU. Modification of a sequence number or destruction of a single TPDU can cause significant disruption even if all PDUs cannot be intercepted because TPDUs received out-of-sequence are held until all in-sequence PDUs are received and are discarded if they are not received within a specified time window.

TP4 allows explicit flow control to regulate the flow of Data TPDUs independently of the flow control in other layers. TP4 procedures include a timeout to compensate for unsignalled loss of TPDUs by the network service provider. Delay of traffic or acknowledgments can be disruptive because timeouts trigger the source host to retransmit unacknowledged TPDUs.

The checksum is optional, and when included, is used to detect corruption of TPDUs by the network service provider. It is subject to modification by an intruder along with other fields. An adversary that chooses to modify traffic must also modify the checksum in order to prevent the PDU from being rejected for transmission errors. An attack of this nature is not trivial. The intruder would have to know the checksum algorithm, then gain access to the traffic as it passes over the network, and finally perform the modifications without being discovered.

Since CLNP is connectionless, no connection is established and all PDUs include security relevant information. CLNP is designed to operate over a homogeneous or heterogeneous set of interconnected subnetworks and can operate end-to-end. The CLNP header includes network source and destination SAPs. Therefore, an adversary can derive the source and destination of the message regardless of whether the transport header is protected. Associating NSAPs with specific network components could be accomplished by reviewing network management documentation or through direct observation of the network to determine which nodes act as sinks for NSAP addresses.

Equally significant are the CLNP options to allow source routing, whereby the originating ES designates the route of the PDU, and route recording, whereby each IS identifies itself in the NPDU header so that the destination ES can review its path. The congestion notification flag can be set by any IS that processes the NPDU. These fields can provide an eavesdropper with the ability to derive special routing policies and security needs of the source host as well as information about the network as a whole. Knowledge of these routing policies can help an adversary determine which

subnetworks to target for traffic analysis. Collateral information for a specific system might also reveal that the setting of the congestion notification flag corresponds to a particular system mission or activity.

CLNP PDUs can include a priority parameter which might be used by an adversary to gain some insight into the importance of the traffic regardless of whether the transport header is protected. There is also a lifetime field in the header that is used to eliminate expired PDUs from the network. An adversary could modify the lifetime field in order to flood a network or to cause messages to expire before they arrive at their destination and still maintain the normal traffic flow out of the adversarial station. If an adversary significantly lowers the lifetime counter for one PDU segment such that the segment expires, it will cause the destination host to discard all segments of that PDU when the timer expires and the one segment has not been received.

Originators can assign security levels (i.e., labels) to CLNP PDUs. CLNP is not designed as a security protocol and it does not specify the way in which protection services are to be provided; it provides only for the encoding of security information in the PDU header and leaves implementation specifics to the system designer. If the local implementation is sound, CLNP may be able to provide some level of security. However, if an adversary can modify the CLNP security label, they could cause incorrect routing decisions and compromise of classified traffic. Another security relevant field is the checksum. It is used to detect corruption of CLNP PDUs and is subject to modification by an intruder if it is not also afforded confidentiality and integrity protection. Other Network Layer protocols (i.e., NLSP and SP3), on the other hand, are designed with security as the primary goal. They can protect the CLNP PDU, including the security label and other security-relevant information, through the application of confidentiality and integrity services.

CLNP performs segmentation when the PDU is larger than the maximum SDU size supported by the underlying service. Segmentation can hide the length of the NPDU if individual segments are routed differently over the network. Masking the length of the message helps to mask the type of message being transmitted.

Currently, the only security relevant information in the LLC header is address information. The addresses are link source and destination SAPs that identify how the PDU is to be routed within the source and destination host workstations, or to which terminal the PDU is to be routed by the destination concentrator. If the adversary is capable of intercepting the traffic and modifying it before other stations receive it, as is the case with a ring topology, the addresses can be changed to cause disruption. However, to avoid detection the adversary is more likely to operate in promiscuous mode to passively monitor all traffic on the LAN. (When a station operates in promiscuous mode, it accepts all frames sent over the LAN.) This will allow the adversary to be aware of unusual traffic loads for protocol entities within a workstation or for the terminals associated with a concentrator.

MAC frames (CSMA/CD and FDDI) include very similar protocol control information. In both protocols, the source and destination station addresses are shown.

This will allow the adversary to be aware of unusual traffic loads and particular messages being passed between specific stations. Both CSMA/CD and FDDI allow the frame to be broadcast to all stations by setting the destination address to a specified sequence. The length of the LLC PDU is shown in the CSMA/CD frame and can be derived in the FDDI frame by counting the entire frame and subtracting the other fields. Both protocols include a FCS field for integrity. Modification of any other field will usually require that the FCS also be modified to prevent the PDU from being discarded for transmission errors.

Associating MAC addresses with specific stations could be accomplished by reviewing network management documentation (including IEEE standards for globally assigned addresses), or through direct observation of the network to determine which stations act as sinks for MAC addresses.

Other items that a traffic analyst can derive by monitoring traffic are time of transfer and frequency of transmission. [MUFTIC 93] These may, under the right conditions, indicate that a known mission is under way, that a known message has been transmitted, or other compromising facts.

Figure 4.2-2 shows how security protocols at the Transport, Network, and Data Link Layers can hide and protect upper layer header information by encapsulating the headers in encrypted security envelopes. **Figure 4.2-2(a)** shows a protocol stack that includes the Transport Layer Security Protocol (TLSP) or Security Protocol 4 (SP4) at Layer 4, or the Network Layer Security Protocol (NLSP) or Security Protocol 3 (SP3) at the top of Layer 3. These security protocols are mutually exclusive and provide essentially the same services, so only one is implemented in a given stack. All four security protocols use an integrity check value (ICV) and encryption to encapsulate the TP4 and upper layer headers as well as the userdata. All four provide end-to-end security. In addition, NLSP can provide data padding for traffic flow confidentiality. NLSP and SP3 can also provide host-to-gateway or gateway-to-gateway encryption, which is defined in this report as a form of link encryption that applies to a portion of the internetwork. All four protect much of their own headers with the ICV and encryption, leaving no security relevant information in the clear. Only derived information, such as transmission time and frequency can be obtained from the encrypted security envelope by an observer.

Figure 4.2-2(b) shows that NLSP can be implemented below CLNP to also protect Network Layer parameters as well as provide traffic flow confidentiality services. NLSP can include source routing and route recording parameters in the NLSP QOS parameters of the UNITDATA primitive and pass them to the underlying network as QOS parameters. Otherwise, the CLNP source routing and record routing fields will be encapsulated by NLSP and be prevented from being used for the part of the route between the source and destination NLSP entities. [ISO 92B] *(Note: SP3 can also be implemented below CLNP, but is designed to operate above it. Route recording and source routing are QOS parameters that may be included in the SP3I protected header, depending on local policy. [NIST 90])*

802.3/FDDI Header	LLC Header	CLNP Header	**TLSP/SP4/ NLSP/SP3 Header**	TP4 Header	SH	PH	AH	
• source address • dest address within the LAN • length (of LLC PDU) (FDDI: derived from delimiters) • checksum (FCS)	• link SSAP • link DSAP	• network SSAP • network DSAP • source routing • route record • congestion notification • priority • lifetime • security level • segment length • checksum	• no security relevant information in the clear					Application Data

(a) LAN Stack with Security Protocol at Layer 4 or Top of Layer 3

802.3/FDDI Header	LLC Header	**NLSP Header**	CLNP Header	TP4 Header	SH	PH	AH	
• source address • dest address within the LAN • length (of LLC PDU) (FDDI: derived from delimiters) • checksum (FCS)	• link SSAP • link DSAP	• no security relevant information in the clear						Application Data

(b) LAN Stack with Security Protocol at Middle of Layer 3

802.3/FDDI Header	**SDE Header**	LLC Header	CLNP Header	TP4 Header	SH	PH	AH	
• source address • dest address within the LAN • length (of SDE segment) (FDDI: length derived) • checksum (FCS)	• no security relevant information in the clear							Application Data

(c) LAN Stack with Security Protocol at Layer 2

Figure 4.2-2. Reduced Exposure due to Implementation of Security Protocols

Figure 4.2-2(c) shows a protocol stack that includes SDE at Layer 2. SDE is effective in encapsulating all of the LLC through Application Layer headers, as well as all security-relevant parameters in its own header. Security at the Data Link Layer provides excellent protection within a LAN or among LANs that are interconnected by secure bridges. Since all stations on a LAN can monitor all traffic on the LAN, the use of SDE is superior to the use of Layer 3 or 4 security protocols from the standpoint of traffic flow confidentiality.

If the PDU must be routed over an internetwork, the SDE envelope is removed to allow Network Layer processing. Therefore, all the headers are again vulnerable while the PDU is being processed at the IS and beyond if a security protocol is not applied before the PDU leaves the IS. To avoid a vulnerability of this nature, the SDE protocol entities must be placed either at the ES or at bridges to the secure subnetwork where the ES is located.

In some internetworking environments, it may be advisable to use an end-to-end security protocol, as well as SDE from the source host to the bridge and from the bridge to the destination host. The informative annex to IEEE Standard 802.10 suggests that *"it is desirable to protect information at both the highest possible point in the protocol stack (i.e., the Application Layer) and any layers at which subnetworks and routing are implemented."* [IEEE 93A] This is an important point. The Application Layer can selectively provide security to the data that is deemed sensitive and can apply that security in an end-to-end manner which prevents the possibility that an Intermediate System might compromise the data. At the same time, the lower layers can apply security, including traffic flow confidentiality, to all traffic that passes across a high risk link. The standard continues, *"The Data Link Layer of LANs exhibits subnetwork and routing functions similar to those of the Network Layer."* This is also an important point to remember when determining the best methods for applying security to LANs.

4.3 Security Relevant Information in a WAN-Oriented Stack

The OSI stack being considered in this section includes the connection-oriented X.25 Packet Level Protocol and Link Access Procedures - B (LAPB) which are used for WAN connectivity. It also includes the ISO 8073 Connection Oriented Transport Protocol, Class 1 (TP1), as illustrated in **Figure 4.3-1(a)**. A variant is to add ISO 8473-1 Connectionless Network Protocol (CLNP) as the Subnetwork Independent Convergence Protocol (SNICP) operating above X.25 to support internetworking, as illustrated in **Figure 4.3-1(b)**.

The TP1 Connection Request PDU identifies the transport SSAP and DSAP and establishes transport source and destination connection references that are visible in all TPDUs. So, as with TP4, an adversary can derive the source and destination of all TP1 message traffic.

LAPB Header	X.25 Header	TP1 Header	SH	PH	AH	
• length of X.25 segment (derived from LAPB header delimiters) • sequence no. • checksum (FCS)	• network SSAP (setup, clear, & registration PDUs only) • network DSAP (same PDUs) • logical channel number • sequence no.	• transport SSAP • transport DSAP • connection ref. • priority • security label • segment length • sequence no.				Application Data

(a) WAN Stack without CLNP

LAPB Header	X.25 Header	CLNP Header	TP1 Header	SH	PH	AH	
• length of X.25 segment (derived from LAPB header delimiters) • sequence no. • checksum (FCS)	• network SSAP (setup, clear, & registration PDUs only) • network DSAP (same PDUs) • logical channel number • sequence no.	• network SSAP • network DSAP • source routing • route record • congestion notification • priority • lifetime • security level • segment length • checksum	• transport SSAP • transport DSAP • connection ref. • priority • security label • segment length • sequence no.				Application Data

(b) WAN Stack with CLNP

Figure 4.3-1. WAN Security Relevant Parameters Exposed to Interception

The TP1 Connection Request PDU also includes priority, transit delay, and protection (could specify security label) parameters for the connection, but provides no acknowledge time parameter. TP1 is not designed as a security protocol and it does not specify the values for the priority and protection parameters; it provides only for the encoding of security information in the Connection Request PDU and leaves implementation specifics to the system designer. If the local implementation is sound, TP1 may be able to provide some level of security. However, if an adversary can modify the TP1 security label or priority for the connection, they could cause disruption, incorrect routing decisions, and compromise of classified traffic. Other Transport Layer protocols (i.e., TLSP and SP4), on the other hand, are designed with security as the primary goal. They protect the TP1 PDU, including the priority and security label parameters, through the application of confidentiality and integrity services.

TP1 does not provide all of the services that TP4 provides because TP1 is intended for use over medium quality network connections *(those that have acceptable residual error rates — that is, a low percentage of lost, incorrect, or duplicated PDUs — but unacceptable signaling failure rates — that is, insufficient recovery and resequencing)* that provide more services than the low quality network connections

(those that have unacceptable residual error rates and unacceptable signaling failure rates) over which TP4 is intended to operate.

TP1 performs TSDU segmentation and can split a transport connection over multiple network connections, as can TP4. Sequence numbers are assigned to each Data TPDU (i.e., to each segment of the TSDU). Consequently, delay of one TPDU can cause significant disruption since other TPDUs will be received out-of-sequence and will be discarded, requiring retransmission.

TP1 does not provide flow control or checksum capabilities. Therefore, modification of TPDUs is easier with TP1 than with TP4.

When CLNP is implemented as a Subnetwork Independent Convergence Protocol with connection-oriented protocols, it is formatted in the same manner as when it is implemented with connectionless mode protocols. Therefore, the same security relevant fields (i.e., network source and destination SAPs, source routing and route recording lists, congestion notification flag, priority, lifetime, security level, segment length, and checksum) are present in the header.

Only the X.25 setup and clear PDUs (Call Request, Call Accepted, Incoming Call, Call Connected, Clear Request, Clear Indication, DTE Clear Confirmation, and DCE Clear Confirmation) and the Registration Request and Registration Confirmation PDUs include network SSAP and DSAP fields. However, they also include a logical channel number (LCN) which is included in all other PDUs, and which makes it possible for an adversary to identify the SAP addresses of Data PDUs if the call setup PDU was previously intercepted.

X.25 performs segmentation of messages into small packets, appends sequence numbers to the packets, and transmits the packets across diverse routes on the network. X.25 does not provide source routing and cannot therefore guarantee that packets will take diverse routes. Even if CLNP is implemented over X.25 to provide source routing, CLNP will not be aware of the X.25 packets (i.e., segments of the CLNP PDU) and will not be able to provide individualized source routing.

As with other sequencing protocols, destruction of one X.25 Data packet can cause more serious disruption because later packets will be received out-of-sequence and flow control will inhibit continued transmission until the missing packet is received at the destination. Flow control packets (Receive Ready, Receive Not Ready, and DTE Reject) provide the traffic analyst with information about the capability of the receiving station. This information may be useful at a later date should the adversary wish to cause congestion of the receiving station.

The structure of LAPB is similar to that of Type 2 LLC. With LAPB, there are no addresses. However, an eavesdropper would know that the protocol connects only one DCE and one DTE, and would therefore know the addresses through collateral information. The destination address field identifies whether the frame is a command or response and whether it is a single link or multilink operation.

LAPB Information PDUs contain send and receive sequence numbers that are used for flow control. LAPB frames also include a frame check sequence field for integrity. Modification of any other field would require that the frame check sequence also be modified to prevent the frame from being discarded for transmission errors.

Figure 4.3-2 shows how security protocols at the Transport and Network Layers can hide and protect upper layer header information by encapsulating the headers in security envelopes.

Figure 4.3-2(a) shows a protocol stack that includes TLSP or SP4 at Layer 4, or NLSP or SP3 at the top of Layer 3. These security protocols are mutually exclusive and provide essentially the same services, so only one is implemented in a given stack. All four security protocols use an integrity check value (ICV) and encryption to encapsulate the TP4 and upper layer headers as well as the userdata. All four provide end-to-end security. In addition, NLSP can provide data padding for traffic flow confidentiality. NLSP and SP3 can also provide host-to-gateway or gateway-to-gateway encryption, which is defined in this report as a form of link encryption that applies to a portion of the internetwork. All four protect much of their own headers with the ICV and encryption, leaving no security relevant information in the clear. Only derived information, such as transmission time and frequency can be obtained from the encrypted security envelope by an observer.

Figure 4.3-2(b) shows the same security implementation, but with CLNP in the stack. The security protocols implemented at Layer 4 or the top of Layer 3 *will not* protect the CLNP header, and thus will not protect the CLNP addresses and other CLNP header information. **Figure 4.3-2(c)** shows that NLSP can be implemented below CLNP to also protect CLNP parameters. However, does not protect an X.25 header (of particular interest are the X.25 source and destination SAPs), nor the LAPB header, of course.

The use of SDE at Layer 2 is not supported in WAN stacks. Therefore, none of the network routing information in the X.25 header can be protected without full period encryption at the Physical Layer.

LAPB Header	X.25 Header	**TLSP/SP4/ NLSP/SP3 Header**	TP1 Header	SH	PH	AH	
• length of X.25 segment (derived from LAPB header delimiters) • sequence no. • checksum (FCS)	• network SSAP (setup, clear, & registration PDUs only) • network DSAP (same PDUs) • logical channel number • sequence no.	• no security relevant information in the clear					Application Data

(a) WAN Stack with Security Protocol at Layer 4 or Top of Layer 3

LAPB Header	X.25 Header	CLNP Header	**TLSP/SP4/ NLSP/SP3 Header**	TP1 Header	SH	PH	AH	
• length of X.25 segment (derived from LAPB header delimiters) • sequence no. • checksum (FCS)	• network SSAP (setup, clear, & registration PDUs only) • network DSAP (same PDUs) • logical channel number • sequence no.	• network SSAP • network DSAP • source routing • route record • congestion notification • priority • lifetime • security level • segment length • checksum	• no security relevant information in the clear					Application Data

(b) WAN/CLNP Stack with Security Protocol at Layer 4 or Top of Layer 3

LAPB Header	X.25 Header	**NLSP Header**	CLNP Header	TP1 Header	SH	PH	AH	
• length of X.25 segment (derived from LAPB header delimiters) • sequence no. • checksum (FCS)	• network SSAP (setup, clear, & registration PDUs only) • network DSAP (same PDUs) • logical channel number • sequence no.	• no security relevant information in the clear						Application Data

(c) WAN/CLNP Stack with Security Protocol at Middle of Layer 3

Figure 4.3-2. Reduced WAN Exposure due to Implementation of Security Protocols

This Page Intentionally Left Blank

Section 5

Analysis of Traffic Flow Confidentiality Options

This Page Intentionally Left Blank

5.0 Analysis of Traffic Flow Confidentiality Options

The OSI Security Architecture Standard, ISO 7498-2, identifies the layers at which traffic flow confidentiality services can be provided in the OSI RM — namely Layers 7, 3, and 1. It says:

- **Application Layer** – a limited traffic flow confidentiality service can be supported by the use of a traffic padding mechanism at the Application Layer in conjunction with a confidentiality service *(i.e., an encipherment mechanism)* at a lower layer. Encipherment mechanisms applied to data transfers, when located in the upper layers, will be contained in the Presentation Layer.
- **Network Layer** – the traffic flow confidentiality service is achieved by a traffic padding mechanism, in conjunction with a confidentiality service at or below the Network Layer and/or routing control.

  If traffic padding is used in conjunction with an encipherment mechanism in the Network Layer (or a confidentiality service from the Physical Layer), then a reasonable level of traffic flow confidentiality may be achieved.
- **Physical Layer** – The traffic flow confidentiality service takes two forms:

  (1) Full traffic flow confidentiality which can be provided only in certain circumstances, e.g. two-way simultaneous, synchronous, point-to-point transmission; and

  (2) Limited traffic flow confidentiality which can be provided for other types of transmission, e.g. asynchronous transmission.

  These security services are restricted to passive threats and can be applied to point-to-point or multi-peer communications.

Many of the security mechanisms discussed in previous sections provide protection against active threats as well. To be effective, multiple mechanisms must be implemented in a cooperative manner. It should be noted that in some environments, traffic padding provided by the traffic flow mechanisms at Layers 7 and 3 may also be supported by encryption at Layers 4 and 2.

Different approaches are needed for traffic flow confidentiality in a WAN than for traffic flow confidentiality in a LAN. **Section 5.1** discusses options for a WAN and **Section 5.2** discusses options for a LAN.

5.1 WAN Traffic Flow Confidentiality Options

Data padding performed at the Application Layer is the first step in effectively concealing message sizes. An application that exchanges formatted messages (such as personnel records, casualty reports, situation reports, emergency action messages, and ship movement reports) may be encrypted so that an adversary cannot determine the contents. Encryption alone still reveals general information if the adversary can determine what type of message has been sent, and how many. Padding will help to conceal the message type. When data padding is performed, it must be hidden by end-to-end encryption.

End-to-end encryption can be provided by application processes or by correspondent protocol entities in Layers 4 through 7 located at the source and destination hosts. In addition, security protocols located at the top of Layer 3 can provide end-to-end encryption service for the Transport Layer. The OSI Security Architecture, ISO 7498-2, provides for traffic flow confidentiality only at Layers 7, 3, and 1 and requires that the confidentiality process (e.g., encryption) be applied below Layer 7 and below the padding process. *Therefore, end-to-encryption as a confidentiality process to support traffic flow confidentiality can only occur in Layers 3 and 6, and must occur in conjunction with the padding process.* In conclusion, when data padding is performed at the Application Layer, it must be hidden by end-to-end encryption provided at the Presentation Layer.

Timing techniques to delay low priority messages can be employed at the Application Layer when there is heavy traffic so the load stays at an even level in order to conceal the fact that an unusually high number of messages, or a peculiar pattern of messages, are being transmitted. The purpose is to conceal that a particular mission or activity may be underway, as indicated by the heavy or peculiar traffic loads. This is difficult and costly to implement since multiple mechanisms must be developed for specific instances of communication in specific applications.

Dummy traffic can be generated between two hosts at the Application Layer when traffic loads are low. The dummy traffic can be removed when loads increase in order to help camouflage the fact that heavy traffic loads are occurring. This mechanism will congest the network if it is used extensively. Therefore, it should be applied sparingly at carefully selected peer-entities.

End-to-end PDU ***segmentation*** and ***route control*** mechanisms are effective at the Transport Layer. Both TP1 and TP4 perform segmentation, and TP4 has the ability to split a transport connection to allow use of multiple network connections. However, TP4 cannot specify the path that the segments will follow through the network. TLSP or SP4 can be applied below TP1 and TP4 to encapsulate all of the headers above it with integrity checking and ***end-to-end encryption.***

All of the security features discussed so far can also be implemented at the Network Layer. When many applications are used, data padding at the Application Layer provides limited security and should be performed at a lower layer instead (e.g., Network Layer) so that it can protect traffic for all applications between two hosts that are related through a security association.

The only security protocol that explicitly provides traffic flow confidentiality services is the Network Layer Security Protocol (NLSP), and it is limited in application when it is implemented at the top of the Network Layer because it cannot provide security for any Network Layer headers which contain routing information if it is placed above them. NLSP specifically provides a ***data padding*** field (called *traffic padding* field) for the purpose of traffic flow confidentiality. NLSP also provides integrity checking and ***encipherment*** of the NSDU to complete the traffic flow confidentiality service within one protocol. Security Protocol 3 (SP3) never explicitly discusses traffic flow confidentiality, but it does have a padding field and it does provide encapsulation through integrity checking and encipherment. Both NLSP and SP3 may be implemented below CLNP to protect both the CLNP and the Upper Layer headers. Of course, it will not protect an X.25 header which is implemented below it at the Subnetwork Access Protocol (SNAcP) sublayer.

Dummy traffic can be generated between two end systems or any segment of a network to help camouflage heavy traffic loads at the Network Layer. This mechanism will congest the network if it is used extensively for distances greater than one point-to-point link. X.25 can effectively implement this mechanism between selected DCEs and their associated DTEs.

NLSP and SP3 services can be applied end-to-end, or across a link or links of the network. Both CLNP and X.25, as well as NLSP perform NPDU ***segmentation*** and can route the segments over diverse routes. In addition, LAPB is able to route Data Link SDUs over multiple independent physical circuits. The Network Layer is the only layer that is able to implement strict ***route control***. It does this through use of the CLNP source routing option. It is also able to avoid congested nodes through use of the CLNP congestion notification option.

5.2 LAN Traffic Flow Confidentiality Options

For WANs, the Data Link and Physical Layer entities always lie across a physical link. For LANs, the situation is more complex. LANs can be directly connected through a local bridge or connected over a link with a pair of remote bridges. Bridges are relays that process PDUs up to the Data Link Layer. When a collection of LANs is connected through bridges, it is possible for the entities that encipher and decipher the data to lie within either the hosts or the bridges. The Data Link Layer can thus provide either link or end-to-end encryption for an internetwork consisting of LANs. [SSI 92]

Traffic flow confidentiality is generally better at the LLC and Network Layers than at the Physical Layer (from the standpoint of authorized stations rather than outsiders) because intermediate stations on the LAN will observe all MAC and Physical Layer traffic but may be denied the opportunity to monitor LLC or Network Layer headers if the corresponding LLC and Network protocol entities are located in the end systems or more distant intermediate stations. Traffic padding (both ***data padding*** and the generation of ***dummy traffic)*** at the Network Layer followed by encryption, also at the Network Layer, provides a strong level of traffic flow confidentiality. However, since nodes on LANs share the transmission media, traffic padding will congest the network.

The Secure Data Exchange Protocol (SDE) operates at the Data Link Layer and performs ***segmentation***, ***data padding***, and ***encapsulation*** and can therefore provide traffic flow confidentiality within a LAN. What remains exposed to observation by other nodes on the LAN are the MAC addresses, and time and frequency of transmission. ***Traffic padding*** (i.e., generation of spurious traffic) can be provided at this layer, but again has the side effect of causing congestion on the LAN.

A mechanism that offers a high degree of protection from wiretapping of the link between two remote bridges which are in close proximity, such as might be found on a ship or within a building, is a point-to-point ***Protected Distribution System***. This would exclude outsiders from gaining the opportunity to observe traffic on the LAN and would limit the scope of protection to the authorized nodes on the LAN. When the remote bridges are geographically remote, requiring radio wave or satellite communications, ***full period encryption*** at the Physical Layer is the recommended mechanism to provide confidentiality.

Section 6

Conclusions and Recommendations

This Page Intentionally Left Blank

6.0 Conclusions and Recommendations

The conclusions and recommendations of this study fall into the following categories:

- Protocol control information exposed to interception
- Traffic flow confidentiality options
- End-to-end encryption and traffic flow confidentiality recommendations.

6.1 Protocol Control Information Exposed to Interception

The security protocols that can provide end-to-end encryption operate at the Network Layer and above. They hide the userdata and upper layer headers from when they leave the source host until when they arrive at the destination host. However, they are not able to protect the lower layer headers, since those headers are applied after the end-to-end encryption service is provided.

The resultant lower layer header information is at risk of being observed, modified, or duplicated by an adversary. Those headers were analyzed to determine what security information is contained in them or might be derived from them by a traffic analyst. Security relevant fields in the protocol headers are shown in **Figure 6.1-1**.

The Transport Layer and above provide end-to-end communications and identify the actual source and destination hosts. The connection oriented transport protocol (TP1 and TP4) headers include the transport source and destination SAPs, the segment length, sequence number, and priority. In addition, TP4 includes flow control, acknowledgment time, and checksum parameters. Traffic analysts can use this information to recognize when particular activities are underway at the source and destination organizations.

TP1 and TP4 also perform segmentation of transport service data units in order to meet size limitations. Segmentation has a positive side effect in that it limits the amount of data that is available to an eavesdropper, particularly when the PDUs are transmitted through the network over different routes. If padding and encryption are performed in the Application and Presentation Layers, the adversary may be able to derive information about the PDU type. However, if lower layer security protocols are used to encapsulate the TPDU segments, then an eavesdropper cannot determine the original PDU length or type, what application it is associated with, the frequency of transmission of this type of PDU, and other factors. The security protocols that would be applied below the connection oriented transport protocol are TLSP or SP4 at the Transport Layer, or NLSP or SP3 at the top of the Network Layer. These are shown in **Figure 6.1-2** along with other placement options.

802.3/FDDI Header	LLC Header	CLNP Header	TP4 Header	SH	PH	AH	
• source address • dest address within the LAN • length (of LLC PDU) (FDDI: derived from delimiters) • checksum (FCS)	• link SSAP • link DSAP	• network SSAP • network DSAP • source routing • route record • congestion notification • priority • lifetime • security level • segment length • checksum	• transport SSAP • transport DSAP • connection ref. • priority • ack time • security label • segment length • sequence no. • flow control • checksum				Application Data

(a) LAN Stack

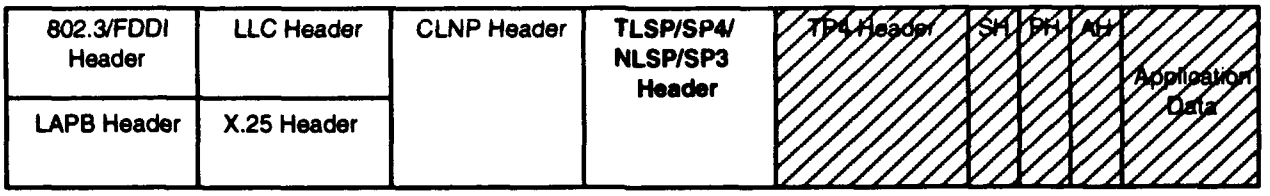
LAPB Header	X.25 Header	TP1 Header	SH	PH	AH	
• length of X.25 segment (derived from LAPB header delimiters) • sequence no. • checksum (FCS)	• network SSAP (setup, clear, & registration PDUs only) • network DSAP (same PDUs) • logical channel number • sequence no.	• transport SSAP • transport DSAP • connection ref. • priority • security label • segment length • sequence no.				Application Data

(b) WAN Stack without CLNP

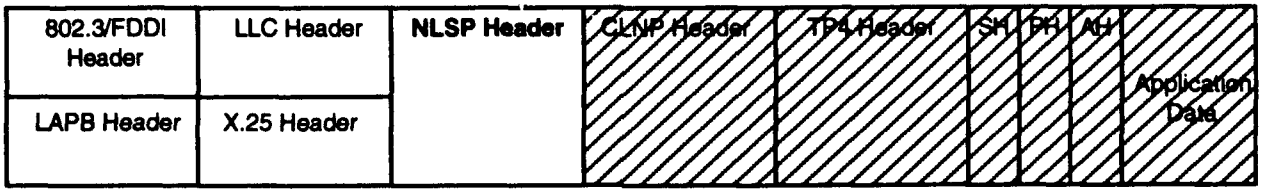
LAPB Header	X.25 Header	CLNP Header	TP1 Header	SH	PH	AH	
• length of X.25 segment (derived from LAPB header delimiters) • sequence no. • checksum (FCS)	• network SSAP (setup, clear, & registration PDUs only) • network DSAP (same PDUs) • logical channel number • sequence no.	• network SSAP • network DSAP • source routing • route record • congestion notification • priority • lifetime • security level • segment length • checksum	• transport SSAP • transport DSAP • connection ref. • priority • security label • segment length • sequence no.				Application Data

(c) WAN Stack with CLNP

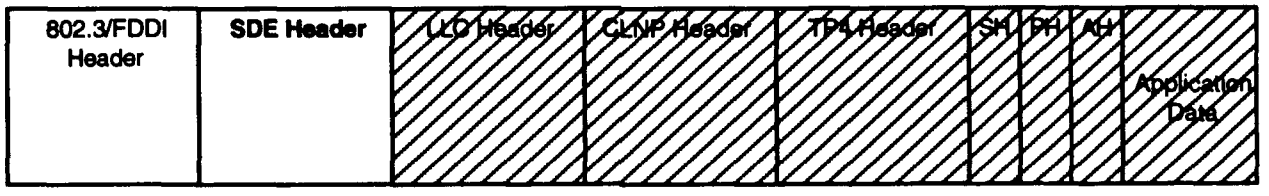
Figure 6.1-1. Security Relevant Parameters Exposed to Interception



(a) Security Protocol at Layer 4 or Top of Layer 3



(b) Security Protocol at Middle of Layer 3



(c) Security Protocol at Layer 2

Figure 6.1-2. Placement of Security Protocols

If CLNP (or IP) is used at the Network Layer, its header may contain the source and destination network SAPs, the segment length, priority, security level (i.e., label), PDU lifetime, and checksum parameters, and network source routing list, a network route recording list, and a network congestion notification flag. Even when the transport header is protected, traffic analysts can use this network header information to recognize when particular activities are underway at the source and destination organizations, when particular messages are sent, and how often those message are sent. CLNP headers can be concealed in some networking environments by implementing NLSP or SP3 below CLNP, as illustrated in **Figure 6.1-3**.

In this example, a subnetwork is connected to an internetwork through a router to form a larger internetwork. The subnetwork and internetwork are controlled by different administrative authorities and use different security mechanisms for protection. The subnetwork is an X.25 WAN that uses NLSP to provide encryption between Host A and Router B (*link encryption* since it is not ES-to-ES, but end-to-end encryption within the context of the X.25 WAN). The internetwork is comprised of subnetworks (LANs and WANs) that all use some form of link encryption. All of the hosts and routers associated with the X.25 WAN and internetwork are identified by common global NSAPs associated with CLNP.

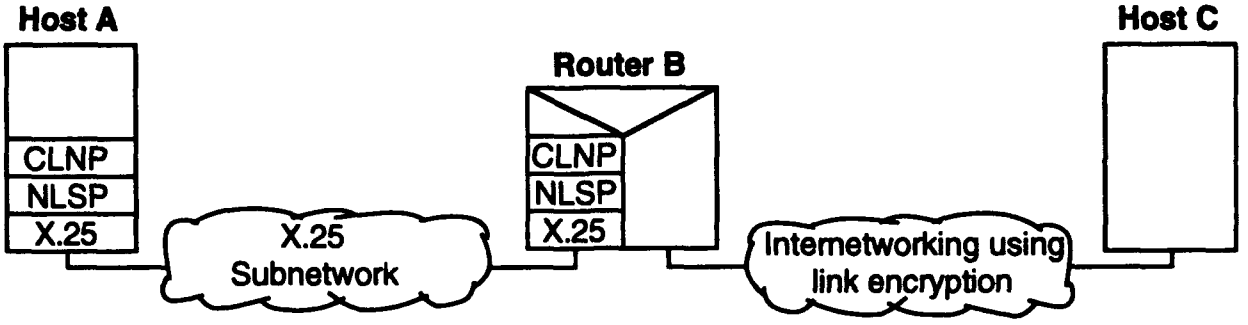


Figure 6.1-3. Concealment of CLNP headers by NLSP

To send traffic from Host A (which is connected to the X.25 WAN) to Host C (which is connected to the internetwork), Host A forms a CLNP header that contains the destination NSAP for Host C. It then passes the CLNP header and data down to NLSP which encrypts them both and passes the results (SDU) down to the X.25 layer. The X.25 protocol entity creates an X.25 header that contains the local X.25 DTE address of Router B, since the destination NSAP (Host C) does not correspond to any host connected to the X.25 WAN (Router B acts as a gateway into the internetwork WAN). The resultant PDU is then sent to Router B using this X.25 header.

When the PDU arrives at Router B, the X.25 header is stripped off and the resultant SDU is passed up to the NLSP layer. NLSP decrypts it and removes its header as well. This reveals the destination NSAP (Host C) to Router B at the CLNP sublayer which uses it to decide which router within the internetwork to forward the SDU to next.

The CLNP destination NSAP continues to be used by routers within the internetwork to forward the SDU to Host C, but is not revealed to outsiders along the way since all of the subnetworks within the internetwork use link encryption. In this environment, CLNP headers are concealed from outsiders that monitor the X.25 subnetwork by using NLSP below CLNP to provide end-to-end encryption within the context of the X.25 network.

Another option is to implement CLNP at the top of the Network Layer for full end-to-end internetworking with a security protocol below it and another CLNP protocol entity below the security protocol to accomplish subnetwork routing.

If X.25 and LAPB are implemented (whether or not there is a security protocol to protect the headers above), they will expose some information that can only be protected at the Physical Layer, since SDE can only be used with LLC. The X.25 header includes network source and destination SAPs (setup and clear, and registration PDUs only), logical channel numbers, and sequence numbers. X.25 does perform segmentation and LAPB can route frames over multiple links. While this may in some cases hide the PDU length and some of the information, it is not a strong form of security and cannot be relied upon. LAPB headers also include X.25 segment length and sequence numbers, and a frame check sequence for integrity.

If LLC is used, SDE can be used to encapsulate the LLC and CLNP headers. LLC displays the link source and destination SAPs. SDE displays no security relevant information.

FDDI and CSMA/CD are implemented below the security protocols analyzed in this study and cannot be protected except through full period encryption at the Physical Layer. Their headers contain the source and destination addresses within the LAN and a frame check sequence. CSMA/CD also identifies the length of the frame. The length of the FDDI frame can be derived from observation.

As illustrated in **Figure 6.1-4**, full period encryption will protect all of the protocol control information at all of the layers (except CSMA/CD because the preamble and start frame delimiter must be sent in the clear).

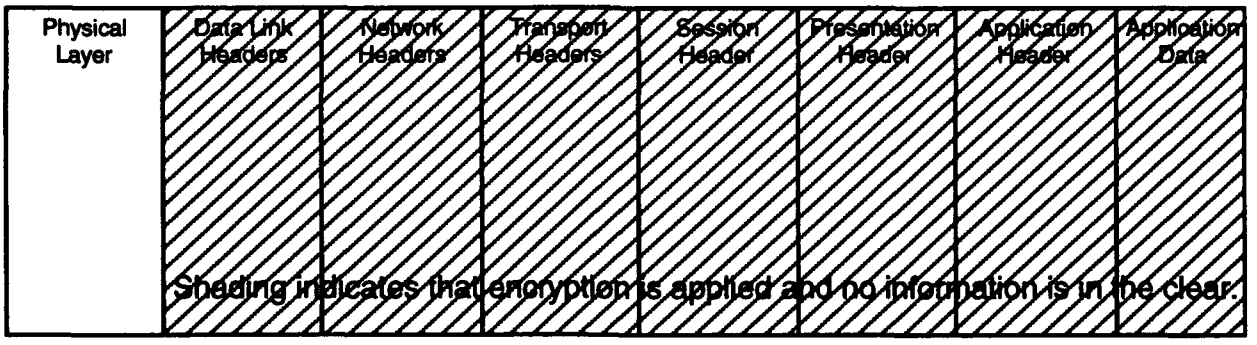


Figure 6.1-4. Full Period Encryption at the Physical Layer

Full period encryption will not protect against an adversary that takes control of an authorized station on a LAN since full period encryption is applied individually across each link and message traffic is decrypted at each intermediate station.

6.2 Traffic Flow Confidentiality Options

The OSI Security Architecture, ISO 7498-2, identifies the layers at which traffic flow confidentiality can be provided: the Application Layer, Network Layer, and Physical Layer. When traffic padding is accomplished at the Application Layer, encipherment will be accomplished at the Presentation Layer after context translation. When traffic padding is accomplished at the Network Layer, encipherment can be accomplished immediately after by the same protocol entity. Full traffic flow confidentiality can only be provided at the Physical Layer in certain circumstances: two-way simultaneous (full-duplex), synchronous, point-to-point transmission. When two-way alternate (half-duplex) transmission is used over a single physical channel, the direction of transmission is still detectable to outsiders as the channel is reversed. When asynchronous channels are encrypted, start and stop bits are still sent in the clear, thereby revealing when characters are transmitted. (This assumes that the ciphertext continues to be transmitted in the asynchronous mode and has not been converted for synchronous transmission.) When a multipoint (broadcast) topology is used, different nodes act as traffic sources at different times. The node acting as a traffic source can still be detected by outsiders when multipoint channels are encrypted. Full traffic flow confidentiality is not effective against active threats unless integrity mechanisms are also utilized. For traffic flow confidentiality to be effective, multiple mechanisms must be implemented in a cooperative manner.

Data padding performed at the Application Layer is the first step in effectively concealing message sizes and types. Data padding can also be accomplished at the Transport, Network, and Data Link Layers, perhaps with less impact because it would not be applied to individual applications. In addition, dummy traffic can be generated between two End Systems or any segment of a network to help camouflage heavy traffic loads. While traffic padding is an important traffic flow confidentiality mechanism, it incurs much overhead because connections must be padded to near capacity in order to conceal when peak traffic actually exists. Since resources are shared, traffic padding of one connection has an adverse affect on all other connections that share those network components. Padding is best suited for selected dedicated routes within an internetwork, and on links between a particular host and a gateway.

Route control is an effective support mechanism to help ensure that traffic is not routed over insecure subnetworks or components. It can and should also be used to disperse PDUs and PDU segments over diverse paths. However, traffic analysts may still be able to recognize when traffic between two particular hosts is high if addresses or PDU types can be identified, even though they cannot observe the full load. Timing techniques to delay low priority messages can be employed when there is heavy traffic so the load appears to stay at an even level.

Although the OSI Security Architecture does not call for traffic flow confidentiality services at the Data Link Layer, SDE can perform segmentation, encapsulation, and in some situations data padding, and can therefore provide limited traffic flow confidentiality within a LAN, or across multiple LANs connected by remote bridges.

What remains exposed to observation by other nodes on the LAN are the MAC addresses, and time and frequency of transmission.

A mechanism that offers a high degree of protection from wiretapping of the link between two remote bridges which are in close proximity is a Protected Distribution System. However, a PDS would not protect traffic from observation by other stations on the LAN. Full period encryption provides a similar service when the remote bridges are geographically remote.

6.3 End-to-End Encryption and Traffic Flow Confidentiality Recommendations

Various end-to-end encryption and traffic flow confidentiality options are appropriate for different environments. In most environments, the processing overhead associated with implementing traffic flow confidentiality is unwarranted.

In those cases where traffic flow confidentiality is warranted, it may be advisable to implement a combination of mechanisms at different layers. As discussed earlier, IEEE Standard 802.10 suggests, *"The security requirements for a particular implementation will determine where the service will be provided. In practice, it is desirable to protect information at both the highest possible point in the protocol stack (i.e., the Application Layer) and any layers at which subnetworks and routing are implemented."* [IEEE 93A] Implementation of traffic flow confidentiality at the Application Layer will allow the user to be selective. In addition, it provides end-to-end (user-to-user) service. By implementing traffic flow confidentiality at a lower layer, traffic flows for the End System as a whole can be masked. In most cases, implementation of one or the other is sufficient, depending on whether traffic flow confidentiality is desired for the entire host or for selective applications on the host, or even selective traffic processed by the application. While traffic flow confidentiality is generally only necessary at either the Application Layer or a lower layer, confidentiality, integrity, and service assurance are more likely to be needed at both levels.

When deciding whether to implement confidentiality services at the Network or Data Link Layers, system architects must consider what type of network is involved. In a WAN, subnetworks and routing are implemented at the Network Layer. Similar subnetwork and routing functions are exhibited at the Data Link Layer in LANs. For these reasons, the following traffic flow confidentiality options are recommended:

- **Application Layer** – when an application processes classified information that is highly desired by an adversary and that information is transmitted over an internetwork where the adversary may have an opportunity to observe, modify, or delay the information, a data padding mechanism should be placed in the Application Layer to disguise the message type and size. Timing techniques should be implemented in the application process to delay low priority traffic during peak traffic periods and dummy traffic should be generated during low traffic load periods so that high loads cannot be identified.

- **Presentation Layer** – end-to-end encryption should be applied in conjunction with the traffic padding mechanism in the Application Layer.
- **Network Layer** – Network Layer mechanisms can be applied to traffic originating from a broad range of applications on the host and are less costly to implement than if they were implemented in each application process or protocol. If a single Application Service Element (ASE) or operating system utility is used to protect all application processes, then implementation costs will be comparable. Data padding, end-to-end encryption, and the generation of dummy traffic should be performed at the Network Layer for most environments, particularly when it is necessary to camouflage all traffic between two hosts or a set of hosts. The use of dummy traffic at the Network Layer should be limited to hosts that require strong traffic flow confidentiality so that the network does not become overly congested. In most cases, it would be better to generate dummy traffic at the Data Link Layer for dedicated links between two stations.

  Additional protocol options that could be implemented at the Network Layer include segmentation, disbursement of the segments, and route control. Route control can only be implemented at the Network Layer. These mechanisms have much less impact on network performance than does the generation of dummy traffic and should be used when portions of the network are outside the controlled environment.
- **Data Link Layer** – The generation of dummy traffic across the link between a DTE and a DCE should be used to hide the true traffic load to and from the End System without causing congestion on the network. Timing techniques should be implemented on the same links as well, and for the same reasons.

  The segmentation, data padding, and encapsulation capabilities of SDE can be used on LANs to hide PCI from other stations that are authorized to connect to the LAN when pairwise unique keys are employed between stations. SDE is also effective between multiple LANs connected by local or remote bridges and can be used to provide end-to-end encapsulation within a LAN internetwork.
- **Physical Layer** – Full period encryption should be used to protect individual point-to-point links. In particular, full period encryption should be used on links between remote bridges that are outside of protected enclosures and protected paths.
- **Physical Installation** – A protected distribution system should be installed to protect cables that traverse areas that are not protected at the level of the data being carried on the network. For example, if two shipboard LANs are installed in areas of a ship that are not adjacent, the cable connecting the remote bridges should be protected by a PDS.

In summary, Application Layer mechanisms should be reserved for those sites or applications that are determined to have traffic profiles which can be used to infer classified missions or information. When traffic flow confidentiality is deemed necessary, the protocol stack should primarily include traffic flow confidentiality services at the Network Layer for internetwork traffic and at the Data Link Layer, when possible, for traffic contained within the LAN.

Traffic flow confidentiality on a link basis should be more widely implemented for the links that connect End Systems to the network. This can be implemented most robustly using full period encryption. An alternative that is feasible for some sites is to use a PDS. The link between LANs that are connected by remote bridges should be protected by full period encryption or a PDS.

It is recommended that research continue so that mechanisms that currently exist to provide these traffic flow confidentiality services can be identified. Four of the security protocols have been standardized in the last six years, and two of them in the last two years. The fifth, IEEE 802.10, is not sufficiently stable to call it standardized, though several vendors are developing prototype implementations. Mechanisms that have been developed to implement these and other protocols should be identified, as should environments for their use. Interoperability between hosts that implement the various security protocols should also be studied. The mechanisms selected to provide traffic flow confidentiality services should support Naval, joint, and combined interoperability requirements.

This Page Intentionally Left Blank

Appendices

This Page Intentionally Left Blank

Appendix A

Acronyms

This Page Intentionally Left Blank

Appendix A

Acronyms

ACK	Acknowledgment
AK	Acknowledgment
ASE	Application Service Element
ASSR	Agreed Set of Security Rules
ATM	Asynchronous Transfer Mode
CL	Connectionless-mode
CLNP	Connectionless Network Protocol
CLNPHDR	CLNP Header
CLTP	Connectionless Transport Protocol
CO	Connection-oriented
COTP	Connection Oriented Transport Protocol
CR	Connection Request
CRC	Cyclic Redundancy Check
CR/CC	Connection Request / Connection Confirm
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DCE	Data Circuit-terminating Equipment
DO	Data Origin
DoD	Department of Defense
DSAP	Destination Service Access Point
DT	Data Protocol Data Unit
DTE	Data Terminal Equipment
E3	End-to-End Encryption
ED	Expedited Data Protocol Data Unit
EHF	Extremely High Frequency
EKE	Exponential Key Exchange
ELF	Extremely Low Frequency
EOT	End of TPDU Mark
ER	Error Protocol Data Unit
ES	End System
ES-ES	End System to End System
ES-IS	End System to Intermediate System
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FSN	Final Sequence Number
FTAM	File, Transfer, Access and Management
GOSIP	Government OSI Profile
HDLC	High-level Data Link Control
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers, Inc.
I/G	Individual / Group Bit
IP	Internet Protocol
IPHDR	Internet Protocol Header

Appendix A – Acronyms (continued)

IS	Intermediate System
IS	International Standard
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System
ISN	Integrity Sequence Number
ISO	International Standards Organization
KM	Key Management
KMP	Key Management Protocol
LAN	Local Area Network
LAPB	Link Access Procedures - B
LCN	Logical Channel Number
LGN	Local Group Number
LLC	Logical Link Control
LSAP	Link Service Access Point
MAC	Mandatory Access Control
MAC	Media Access Control
MAN	Metropolitan Area Network
Mbps	Megabits Per Second
MDF	Management Defined Field
MLP	Multi-Link Procedures
MLS	Multilevel Security
MSDU	MAC Service Data Unit
NAK	Negative Acknowledgment
NES	Network Encryption System
NGCR	Next Generation Computer Resources
NLSP	Network Layer Security Protocol
NPDU	Network Protocol Data Unit
NSA	National Security Agency
NSAP	Network Service Access Point
NSDU	Network Service Data Unit
NSTISSI	National Security and Telecommunications and Information Systems Security Instruction
OSI	Open Systems Interconnection
OSI RM	OSI Reference Model
PCI	Protocol Control Information
PDS	Protected Distribution System
PDU	Protocol Data Unit
PE	Peer-Entity
P/F	Poll / Final Bit
PID	Protocol ID
PMD	Physical Layer Medium Dependent
QOS	Quality of Service
SA	Security Association
SABME	Set Asynchronous Balanced Mode Extended
SAID	Security Association Identifier

Appendix A – Acronyms (continued)

SA-ID	Security Association Identifier
SAP	Service Access Point
SASE	Specific Application Service Element
SBIR	Small Business Innovative Research
SDE	Secure Data Exchange Protocol
SDNS	Secure Data Network System
SDT	Secure Data Transfer
SDU	Service Data Unit
SE TPDU	Security Encapsulation Transport Protocol Data Unit
SILS	Standard for Interoperable LAN/MAN Security
SLP	Single Link Procedures
SMIB	Security Management Information Base
SMT	FDDI Station Management
SNAcP	Subnetwork Access Protocol
SNDCP	Subnetwork Dependent Convergence Protocol
SNICP	Subnetwork-Independent Convergence Protocol
SONET	Synchronous Optical Network
SP3	Security Protocol 3
SP4	Security Protocol 4
SPAWAR	Space and Naval Warfare Systems Command
SSAP	Source Service Access Point
TCP	*Transmission Control Protocol*
TEK	Traffic Encryption Key
TLSP	Transport Layer Security Protocol
TP0	Connection Oriented Transport Protocol, Class 0
TP1	Connection Oriented Transport Protocol, Class 1
TP2	Connection Oriented Transport Protocol, Class 2
TP3	Connection Oriented Transport Protocol, Class 3
TP4	Connection Oriented Transport Protocol, Class 4
TPDU	Transport Protocol Data Unit
TSDU	Transport Service Data Unit
U/L	Universal / Local Bit
UN	Underlying Network
WAN	Wide Area Network
X.25	DCE-to-DTE Packet Level Protocol (CCITT Recommendation X.25)

This Page Intentionally Left Blank

Appendix B

References

This Page Intentionally Left Blank

Appendix B

References

[BLACK 91] U. D. Black, *OSI – A Model for Computer Communications Standards*, Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[CCITT 88] The International Telegraph and Telephone Consultative Committee (CCITT), *Recommendation X.25, Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuits*, 1988.

[FORD 94] W. Ford, *Computer Communications Security – Principles, Standard Protocols and Techniques*, Prentice Hall, Englewood Cliffs, NJ, 1994.

[GASSER 91] M. Gasser, *Building a Secure Computer System*, Van Nostrand Reinhold Company, New York, 1988.

[HALSALL 92] F. Halsall, *Data Communications, Computer Networks and Open Systems*, Third Edition, Addison-Wesley Publishing Company, Reading, Massachusetts, 1992.

[IEEE 93A] Institute of Electrical and Electronics Engineers, *IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS), Currently Contains Secure Data Exchange (SDE) (Clause 2)*, IEEE Standard 802.10-1992, February 5, 1993.

[IEEE 93B] Institute of Electrical and Electronics Engineers, *IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS) Clause 3 — Key Management Protocol*, Unapproved Draft IEEE 802.10c/D2, September 12, 1993.

[ISO 84] International Standards Organization, *Information Processing Systems — Open Systems Interconnection Basic Reference Model*, ISO 7498, October 1984.

[ISO 88] International Standards Organization, *Information Processing Systems — Open Systems Interconnection – Connection Oriented Transport Protocol Specification*, ISO 8073, December 15, 1988.

[ISO 89A] International Standards Organization, *Information Processing Systems—Open Systems Interconnection Basic Reference Model — Part 2: Security Architecture*, ISO 7498-2, February 1989.

Appendix B – References (continued)

[ISO 89B] International Standards Organization, *Information Processing Systems — Fiber Distributed Data Interface (FDDI) — Part 1: Physical Layer Protocol* (PHY), ISO 9314-1, April 1989.

[ISO 89C] International Standards Organization, *Information Processing Systems — Fiber Distributed Data Interface (FDDI) — Part 2: Token Ring Media Access Control,* ISO 9314-2, June 1989.

[ISO 90A] International Standards Organization, *Information Processing Systems — Fiber Distributed Data Interface (FDDI) — Part 3: Physical Layer Medium Dependent (PMD),* ISO 9314-3, October 1990.

[ISO 90B] International Standards Organization, *Information Processing Systems — Local Area Networks — Part 2: Logical Link Control,* ANSI/IEEE Std 802.2, ISO 8802-2, January 12, 1990.

[ISO 90C] International Standards Organization, *Information Processing Systems — Data Communications — X.25 Packet Level Protocol for Data Terminal Equipment,* ISO 8208, 1990; also CCITT Recommendation X.25.

[ISO 92A] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Transport Layer Security Protocol,* ISO/IEC 10736, December 18, 1992

[ISO 92B] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Network Layer Security Protocol,* ISO 11577, November 29, 1992.

[ISO 92C] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Transport Layer Security Protocol (Amendment 1 - Security Association Protocol),* Revised Draft, December 22, 1992.

[ISO 92D] International Standards Organization, *Information Technology — Protocol for Providing the Connectionless-Mode Network Service,* ISO/IEC 8473-1, 1992, identical to CCITT Recommendation X.233.

[ISO 93] International Standards Organization, *Information Processing Systems – Local and Metropolitan Area Networks – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification,* ISO/IEC 8802-3, 1993; commonly known as IEEE 802.3.

Appendix B – References (continued)

[KIRKPAT 91] K. E. Kirkpatrick, "OSI-Based LAN Security Standards," *Handbook of Local Area Networks,* Auerbach Publications, Boston Massachusetts, 1991, pp. 741-753

[LAMBERT 90] P. A. Lambert, "The Lowdown on Lower Layer Security Protocols," *Proceedings of the Sixth Annual Computer Security Applications Conference,* December 1990.

[MUFTIC 93] S. Muftic, et al., *Security Architecture for Open Distributed Systems,* John Wiley & Sons Limited, West Sussex, England, 1993.

[NIST 90] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols,* NISTIR 90-4250, February 1990.

[NIST 91] National Institute of Standards and Technology, *Government Open Systems Interconnection Profile (GOSIP),* FIPS PUB 146-1, April 1991.

[NSTISSI 92] National Security and Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, *National Information System Security (INFOSEC) Glossary,* June 5, 1992.

[SCHLAR 90] S. K. Schlar, *Inside X.25: A Manager's Guide,* McGraw-Hill, New York, New York, 1990.

[SPRAGINS 92] J. D. Spragins, et al, *Telecommunications Protocols and Design,* Addison-Wesley Publishing Company, Reading , Massachusetts, 1992.

[SSI 92] Secure Solutions, Inc., *Placement of Network Security Services for Secure Data Exchange,* SBIR Topic N91-061, November 2, 1992.

[STALLING 85] W. Stallings, *Handbook of Computer Communications Standards – Local Network Standards, Volume 2,* Macmillan Publishers.

This Page Intentionally Left Blank